Internet Fragmentation: An Overview

Edited by: Drake, William J ; Vinton, Cerf G ; Kleinwächter, W

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Future of the Internet Initiative White Paper

Internet Fragmentation: An Overview

January 2016

Future of the Internet Initiative White Paper

Internet Fragmentation: An Overview

William J. Drake
Vinton G. Cerf
Wolfgang Kleinwächter

January 2016

Contents

Preface

The World Economic Forum Annual Meeting 2015 in Davos-Klosters included a session entitled, *Keeping "Worldwide" in the Web*. Participants discussed a number of challenges facing the open global Internet, which has become a key driver of global wealth creation, socio-cultural enrichment and human empowerment in recent decades. Among the top concerns raised was the emerging fragmentation of the Internet along multiple lines due to developments in the technical, governmental and commercial realms. In the months to follow, it became clear that while this fragmentation was of growing concern to many close observers of and participants in the global Internet ecosystem, there was no widespread consensus as to its nature and scope. As such, with the launch of the World Economic Forum's multi-year Future of the Internet Initiative (FII), Internet fragmentation stood out as one of the priority topics meriting exploration in the context of the FII's Governance on the Internet project.

To facilitate the discussion, the Forum invited William J. Drake, who had been a discussion leader at the Annual Meeting session, to organize a small team of experts that could produce a background paper on the subject. This team included Vinton Cerf, widely regarded as a "father of the Internet", and Wolfgang Kleinwächter, a leading figure in global Internet governance institutions. The team's mandate was to contribute to the emergence of a common baseline understanding of Internet fragmentation by undertaking a horizontal mapping of the issues and dynamics involved. That is, its intended value-added would be in presenting a big picture overview of a range of examples illustrating the trend towards fragmentation, rather than in offering finely detailed portraits of any of them.

From the outset of the process, the World Economic Forum engaged a number of interested participants in the FII's Core Community, as well as a group of external experts. The research in progress was discussed both at meetings held in Geneva and New York and on conference calls to engage in dialogue and gather feedback, and over a dozen written replies to the draft version were received as well. All these inputs were taken into consideration by the team of authors. Ultimately though, the views expressed in the paper are solely those of the authors working in their individual capacities, and not necessarily those of their respective organizations, or of the World Economic Forum itself or its Members or Partners.

I would like to thank the authors for their intellectual leadership in developing this analysis, which is an important, new resource for everyone concerned about the evolution of the Internet. I would also like to express appreciation to the informal multistakeholder group of experts who reviewed earlier drafts and provided comments to the authors. The Forum particularly wishes to recognize the leadership and support of the trustees and partners of the Global Challenge Initiative on the Future of the Internet, of which this

workstream is a part, as well as the Initiative's Co-Heads, Mark Spelman and Alex Wong, and its Director, Danil Kerimi.

As a first-cut overview of the fragmentation landscape, this paper will help to set a foundation for further analyses and action-oriented dialogues among FII participants and within the international community at large. It was commissioned for the explicit purpose of providing a more informed basis for the identification and prioritization by all stakeholders of potential areas of collaboration, including the definition of good practices or policy models that can serve as a constructive example for others. A first step down this path will be taken with the Annual Meeting 2016 session on *Internet without Borders*. As the title of this session suggests, the Forum's engagement in this issue area is guided by a conviction that keeping the Internet as open and interoperable as possible is essential if we are to sustain and expand its capacities to promote global well-being in the years ahead.

Richard Samans
Member of the Managing Board

Geneva, January 2016

Executive Summary

A growing number of thought leaders have expressed concerns over the past two years that the Internet is in some danger of splintering or breaking up into loosely coupled islands of connectivity. A number of potentially troubling trends driven by technological developments, government policies and commercial practices have been rippling across the Internet's layers, from the underlying infrastructures up to the applications, content and transactions it conveys. But there does not appear to be a clearly defined, widely shared understanding of what the term, fragmentation, does and does not entail.

The growth of these concerns does not indicate a pending cataclysm. The Internet remains stable and generally open and secure in its foundations, and it is morphing and incorporating new capabilities that open up extraordinary new horizons, from the Internet of Things and services to the spread of block chain technology and beyond. Moreover, the increasing synergies between the Internet and revolutionary changes in other technological and social arenas are leading us into a new era of global development that can be seen as constituting a fourth industrial revolution. But there are challenges accumulating which, if left unattended, could chip away to varying degrees at the Internet's enormous capacity to facilitate human progress. We need to take stock of these, and to begin a more structured dialogue about their nature, scope and distributed collective management.

The purpose of this document is to contribute to the emergence of a common baseline understanding of Internet fragmentation. It maps the landscape of some of the key trends and practices that have been variously described as constituting Internet fragmentation and highlights 28 examples. A distinction is made between cases of technical, governmental and commercial fragmentation. The technical cases generally can be said to involve fragmentation "of" the Internet, or its underlying physical and logical infrastructures. The governmental and commercial cases often more directly involve fragmentation "on" the Internet, or the transactions and cyberspace it conveys, although they also can involve the infrastructure as well. With the examples cited placed in these three conjoined baskets, we can get a holistic overview of their nature and scope and more readily engage in the sort of dialogue and cooperation that is needed.

Section 1: The Nature of Internet Fragmentation

The open Internet provides a baseline approach from which fragmentation departs and against which it can be assessed. Particularly important are the notions of global reach with integrity; a unified, global and properly governed root and naming/numbering system; interoperability; universal accessibility; the reusability of capabilities; and permissionless innovation.

The conventional four-layer technical model of the Internet can analytically supplemented by the addition of a fifth content and transactions layer.

Working definitions are proposed for three forms of fragmentation:

Technical Fragmentation: conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points.

Governmental Fragmentation: Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources.

Commercial Fragmentation: Business practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources.

In each case, fragmentation may vary greatly according to a number of dimensions or attributes. The paper highlights four in particular:

- *Occurrence:* whether a type of fragmentation exists or is a potential
- *Intentionality*: whether fragmentation is the result of deliberate action or an unintended consequence
- *Impact:* whether fragmentation is deep, structural and configurative of large swaths of activity or even the Internet as a whole, or rather more shallow, malleable and applicable to a narrowly bounded set of processes, transactions and actors
- *Character:* whether fragmentation is generally positive, negative, or neutral

Section 2: Technical Fragmentation

When the Internet concept was first articulated, a guiding vision was that every device on the Internet should be able to exchange packets with any other device. Universal connectivity was assumed to be a primary benefit. But there are a variety of ways in which the original concept has been eroded through a complex evolutionary process that has unfolded slowly but is gathering pockets of steam in the contemporary era.

Four issue-areas are reviewed, including Internet addressing, interconnection, naming and security. Within these categories, 12 kinds of fragmentation of varying degrees of significance are identified:

1. Network Address Translation
2. IPv4 and IPv6 incompatibility and the dual-stack requirement
3. Routing corruption
4. Firewall protections
5. Virtual private network isolation and blocking

6. TOR “onion space” and the “dark web”
7. Internationalized Domain Name technical errors
8. Blocking of new gTLDs
9. Private name servers and the split-horizon DNS
10. Segmented Wi-Fi services in hotels, restaurants, etc.
11. Possibility of significant alternate DNS roots
12. Certificate authorities producing false certificates

Section 3: Governmental Fragmentation

The most common imagery of “governmental fragmentation” is of the global public Internet being divided into digitally bordered “national Internets”. Movement in the direction of national segmentation could entail, inter alia, establishing barriers that impede Internet technical functions, or block the flow of information and e-commerce over the infrastructure. Pressure and trends in this direction do exist, as do counter-pressures.

Six issue-areas are reviewed, including: content and censorship; e-commerce and trade; national security; privacy and data protection; data localization; and fragmentation as an overarching national strategy. Within these categories, 10 kinds of fragmentation of varying degrees of significance are identified:

1. Filtering and blocking websites, social networks or other resources offering undesired contents
2. Attacks on information resources offering undesired contents
3. Digital protectionism blocking users’ access to and use of key platforms and tools for electronic commerce
4. Centralizing and terminating international interconnection
5. Attacks on national networks and key assets
6. Local data processing and/or retention requirements
7. Architectural or routing changes to keep data flows within a territory
8. Prohibitions on the transborder movement of certain categories of data
9. Strategies to construct “national Internet segments” or “cybersovereignty”
10. International frameworks intended to legitimize restrictive practices

Section 4: Commercial Fragmentation

A variety of critics have charged that certain commercial practices by technology companies also may contribute to Internet fragmentation. The nature of the alleged fragmentation often pertains to the organization of specific markets and digital spaces and the experiences of users that choose to participate in them, but sometimes it can impact the technical infrastructure and operational environments for everyone. Whether or not one considers commercial practices as meriting the same level of concern as, say, data localization is of course a matter of perspective. Certainly there are significant concerns from the perspectives of many Internet users, activists and competing providers in global markets. As such, the issues are on the table in

the growing global dialogue about fragmentation, and they are therefore discussed here.

Five issue-areas are reviewed, including: peering and standardization; network neutrality; walled gardens; geo-localization and geo-blocking; and infrastructure-related intellectual property protection. Within these categories, 10 kinds of fragmentation of varying degrees of significance are identified:

1. Potential changes in interconnection agreements
2. Potential proprietary technical standards impeding interoperability in the IoT
3. Blocking, throttling, or other discriminatory departures from network neutrality
4. Walled gardens
5. Geo-blocking of content
6. Potential use of naming and numbering to block content for the purpose of intellectual property protection

Section 5: Conclusions

Drawing on the survey of fragmentation examples, a “top 10” set of cases is suggested that are a) fairly pressing or at least worth keeping a close watch of; b) worth examining in greater detail than was possible in this paper; and/or c) potentially amenable to progress through multistakeholder dialogue and collaboration. These are:

- Sustained delays or failure to move from IPv4 to IPv6
- Widespread blocking of new gTLDs
- Significant alternate root systems
- Filtering and blocking due to content
- Digital protectionism
- Local data processing and/or retention requirements
- Prohibitions on the transborder movement of certain categories of data
- Strategies for “national Internet segments” or “cybersovereignty”
- Walled gardens
- Geo-blocking

Taking into account these 10 cases and the preceding discussion, six sets of challenges stand out as being both pressing and particularly amenable to productive analysis and multi-stakeholder dialogue and cooperation:

- Fragmentation as Strategy
- Data Localization
- Digital Protectionism
- Access via Mutual Legal Assistance Treaties (MLATs)
- Walled Gardens
- Information Sharing

Introduction

Internet fragmentation has become a rather hot topic of late. A growing number of thought leaders in government, the private sector, the Internet technical community, civil society and academia have expressed concerns over the past two years that the Internet is in some danger of splintering or breaking up into loosely coupled islands of connectivity. Usually these statements have not been elaborated on at any length, and have offered by way of illustration just a few strains or flash points of tension. Nevertheless, the concern has been picked up and repeated by enough media outlets and mentioned in enough global Internet discussions to transition from a murmur to a near-meme.

The most widely noted catalyst for this emerging discourse has been the June 2013 revelations by Edward Snowden regarding mass surveillance. In the wake of his disclosures, numerous governments began to openly discuss or actively pursue the localization of certain types of data and communication flows within their territorial jurisdictions. But in reality, as significant as these developments have been, they really are only the tip of the iceberg.

For some time now, a number of potentially troubling trends driven by technological developments, government policies and commercial practices have been rippling across the Internet's layers, from the underlying infrastructures up to the applications, content and transactions it conveys. Some of these are of recent vintage, but others are the result of longer-term processes of evolution. The diversity of these trends means that different actors seem to experience and visualize fragmentation differently. In consequence, there does not appear to be a clearly defined, widely shared understanding of what the term does and does not entail.

In a sense, we may be encountering a virtual variant on Miles's law of bureaucratic policy-making, i.e. "Where you stand depends on where you sit." For some in the Internet technical community, fragmentation seems to refer in the first instance to such possibilities as multiple and incompatible root zone files and associated naming and numbering systems; suboptimal changes in the routing architecture; the spread of incompatible technical standards; an increasingly problematic transition from IPv4 to IPv6; and so forth.

In contrast, for some in the business community, the term seems to refer more to variations in national policies that add to the cost of or even block commercial transactions, and especially to new policies and practices that interfere with the transborder flow of data, cloud services, globalized value chains, the industrial Internet, and so on. For many in civil society, fragmentation seems to refer instead to the spread of government censorship, blocking, filtering and other access limitations, as well as to proprietary platforms and business models that in some measure impede end users' abilities to freely create, distribute and access information. Some people even

argue that socio-cultural trends like the increasing linguistic diversity of cyberspace contributes to fragmentation. In short, many people seem to construe fragmentation in ways that reflect their respective experiences and priorities.

This situation is not unexpected, given the number and variety of emerging data points suggesting trends towards fragmentation. Nor is it unprecedented; after all, many other core issues involved in Internet governance and policy today remain contested. Consider for example the ongoing debates about the precise meaning of terms like network neutrality, cybersecurity, or the global public interest. Without shared definitions or at least bounded understandings of what is or is not encompassed by such terms, it can be very difficult to assess emerging trends and the costs and benefits that may be involved, or to evaluate the potential solutions.

So we are in a quandary. There is a growing sense in many quarters that this extraordinary technology that has been a critically important source of new wealth creation, economic opportunity, socio-political development and personal empowerment is experiencing serious new strains and even dangers. This is not to say that some sort of cataclysm is anticipated; the Internet remains stable and generally open and secure in its foundations, and it is morphing and incorporating new capabilities that open up extraordinary new horizons, from the Internet of Things and services to the spread of block chain technology and beyond. Moreover, the increasing synergies between the Internet and revolutionary changes in other technological and social arenas are leading us into a new era of global development that can be seen as constituting a fourth industrial revolution.[1] But it is to say that there are challenges accumulating which, if left unattended, could chip away to varying degrees at the Internet's enormous capacity to facilitate human progress.

We need to take stock of these challenges, and to begin a more structured dialogue about their nature, scope and distributed collective management. No centralized or global intergovernmental response is possible or desirable, given the decentralized character of the Internet that is one of its chief virtues. Effective solutions can only be found through inclusive multistakeholder dialogue and cooperation that is informed by shared understandings of the challenges and the stakes.

Accordingly, the purpose of this paper is to contribute to the emergence of a common baseline understanding of Internet fragmentation. We map the landscape of some of the key trends and practices that have been variously described as constituting Internet fragmentation and highlight 28 examples. We distinguish between cases of technical, governmental and commercial fragmentation. The technical cases generally can be said to involve fragmentation "of" the Internet, or its underlying physical and logical infrastructures. The governmental and commercial cases often more directly involve fragmentation "on" the Internet, or the transactions and cyberspace it

conveys, although they also can involve the infrastructure as well. With the examples cited placed in these three conjoined baskets, we can get a holistic overview of their nature and scope and more readily engage in the sort of dialogue and cooperation that is needed.

It should be noted that while the authors all have strongly held views about the importance of promoting a secure, stable and integrated Internet consistent with the values of open economies and societies as well as fundamental human rights and freedoms, this paper is not intended to argue a strong authorial viewpoint or to offer policy recommendations. Instead, our modest objective is to facilitate discussion among World Economic Forum participants and others in the global community that may have varying viewpoints in the hope that they will work towards the identification of shared priorities and responses.

The paper is organized as follows. Section 1, *The Nature of Internet Fragmentation,* sets out our approach to the subject. Section 2, *Technical Fragmentation,* surveys actual or potential sites of fragmentation in the underlying technological environment that can affect the Internet's functioning. Section 3, *Governmental Fragmentation,* considers the evolving tensions between the territorial sovereign state and the transnational Internet and how these have translated into a complex interplay between fragmentation and harmonization in national policies. Section 4, *Commercial Fragmentation,* turns to the controversies around certain industry practices that some actors view as constituting forms of fragmentation. Finally, Section 5, *Conclusions*, pulls back from the issue survey to offer some observations and options for further work.

1. The Nature of Internet Fragmentation

We begin our inquiry by proceeding in three steps. First, we consider the baseline from which fragmentation is a departure – the open global public Internet. Second, we suggest "working definitions" of technical, governmental and commercial fragmentation that we believe are sufficient to facilitate structured and productive conversation. Finally, we take note of some of the ways in which instances of fragmentation vary from one another, sometimes considerably.

The Open Internet

A useful starting point is to consider what we mean by an unfragmented Internet. What is the baseline from which fragmentation departs and against which it can be assessed?

From a technical standpoint, the original shared vision guiding the Internet's development was that *every device on the Internet should be able to exchange data packets with any other device that was willing to receive them.* Universal connectivity among the willing was the default assumption, and it could be achieved across a network of interconnected networks if the equipment designed by different providers built in interoperability. This means the ability to transfer and make usable data between systems and applications, and it is achieved via the deployment of common technical standards and protocols.[2]

Such interoperability needs to be to be seamlessly coherent on an end-to-end basis. It also needs to be consistent, so that a user's action yields the same response irrespective of the location or service provider involved. Hence, as one leading expert has concluded, from an engineering standpoint, "Fragmentation … encompasses the appearance of diverse pressures in the networked environment that lead to diverse outcomes that are no longer coherent or consistent."[3]

These core features of universal connectivity and interoperability between consenting devices, and the same action yielding the same result each time, are fundamental from a design standpoint. *Actions or conditions that impair this seamless functioning can thus be said constitute technical fragmentation.* But at the same time, this narrow technical definition may be a bit limiting. It does not by itself capture how people use and experience the technology in order to construct digital social formations and engage in information, communication and commercial transactions, or the sorts of political and economic forces that may impede their abilities to do so. In this context, it is useful to recast the notion of an unfragmented Internet in terms of the "open" Internet.

But what is an open Internet? Here again we can step into a lacuna regarding a foundational and valued principle of Internet discourse, design and policy. Over the years, the term “openness” has been paired with many core elements of the information and communication technology environment – open access, open source, open standards, open architecture, open network, open decision processes, and so on – but sometimes fine grained differences of perspective impede the formation of consensus on clear shared meanings. Often people simply answer the question by listing properties of the Internet that they find desirable, although admittedly this is not necessarily the most systematic or neutral approach. A human rights lawyer, a trade economist and a network engineer might each give the term a special shade of meaning based on their respective priorities and experiences.

We cannot attempt to delve deeply into this long-standing question in this paper. For present purposes, it is sufficient to fall back on the approach of listing properties that seem from our vantage points to be integral to a robust conception of “openness“. In its document on “Internet invariants”, the Internet Society has offered a list that is an attractive baseline and is worth quoting at length, in Box 1.

Box 1: The Internet Society’s “Internet Invariants”

Global reach, integrity: Any endpoint of the Internet can address any other endpoint, and the information received at one endpoint is as intended by the sender, wherever the receiver connects to the Internet. Implicit in this is the requirement of global, managed addressing and naming services.

General purpose: The Internet is capable of supporting a wide range of demands for its use. While some networks within it may be optimized for certain traffic patterns or expected uses, the technology does not place inherent limitations on the applications or services that make use of it.

Supports innovation without requiring permission (by anyone): Any person or organization can set up a new service, that abides by the existing standards and best practices, and make it available to the rest of the Internet, without requiring special permission. The best example of this is the World Wide Web – which was created by a researcher in Switzerland, who made his software available for others to run, and the rest, as they say, is history. Or, consider Facebook – if there was a business approval board for new Internet services, would it have correctly assessed Facebook’s potential and given it a green light?

Accessible – it's possible to connect to it, build new parts of it and study it overall: Anyone can "get on" the Internet – not just to consume content from others, but also to contribute content on existing services, put up a server (Internet node) and attach new networks.

Based on interoperability and mutual agreement: The key to enabling inter-networking is to define the context for interoperation – through open standards for the technologies, and mutual agreements between operators of autonomous pieces of the Internet.

Collaboration: Overall, a spirit of collaboration is required – beyond the initial basis of interoperation and bi-lateral agreements, the best solutions to new issues that arise stem from willing collaboration between stakeholders. These are sometimes competitive business interests, and sometimes different stakeholders altogether (e.g. technology and policy).

Technology – reusable building blocks: Technologies have been built and deployed on the Internet for one purpose, only to be used at a later date to support some other important function. This isn't possible with vertically integrated, closed solutions. And, operational restrictions on the generalized functionality of technologies as originally designed have an impact on their viability as building blocks for future solutions.

There are no permanent favourites: While some technologies, companies and regions have flourished, their continued success depends on continued relevance and utility, not strictly some favoured status. AltaVista emerged as the pre-eminent search service in the 1990's, but has long-since been forgotten. Good ideas are overtaken by better ideas; to hold on to one technology or remove competition from operators is to stand in the way of the Internet's natural evolution.[4]

These are all essential aspects of the open Internet environment, and a number of them speak directly to what fragmentation in a broader user-oriented and socio-politically attuned sense of the word entails. *Of particular interest here are the notions of global reach with integrity; a unified, global and properly governed root and naming/numbering system; interoperability; universal accessibility; the reusability of capabilities; and permissionless innovation.* An Internet in which any endpoint could not address any other

willing endpoint and have reliably consistent results; and in which digital resources could not be redeployed to an endless variety of user-defined purposes, including the creation of new applications and services, without needing the permission of an intervening authority – this would be a rather fragmented Internet. It would be one that is robbed of what one leading expert calls “generativity”, or the “system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences”.[5] An open Internet allows creative users to draw on common resources and add to, recombine and customize them in order to design global e-commerce processes and organize value chains, mobilize human rights campaigns, create new products, or socially network with fellow cute cat lovers. Constraints on such usage, in the form of government policies and commercial practices, can cause fragmentation just as much as a technical misfire resulting in inconsistent results.

Working Definitions

Putting users and their freedoms at the centre of the discussion implies the need for an optic that is wider than just whether the infrastructure effectively connects willing devices anywhere and functions consistently each time at each end. The standard engineering description of the Internet is as a four layered stack of functionalities. The lowest is the physical or hardware link layer over which packets are carried, such as Ethernet, Wireless Wi-Fi, dedicated optical telecommunications circuits, or satellite links. Moving up the stack, the network or Internet layer is where the Internet protocol (IP) carries packets from a source to a destination, using the routing protocols to determine the paths taken by the packets. Moving further up, the transport layer comprises protocols for various kinds of data transport, such as sequenced and assure delivery of data using the Transmission Control Protocol (TCP), or the User Datagram Protocol (UDP) for real-time but not necessarily sequenced or guaranteed delivery. Each IP packet carries an indication of which protocol is to be used to handle the contents or payload of each Internet packet. Finally, at the top one finds the applications layer where utility protocols such as File Transport Protocol (FTP), Hypertext Transfer Protocol (HTTP), Simple Mail Transport Protocol (SMTP), and many others reside.

Social analysts often add on top of these four technology layers what they variously call a content, social, or transactional layer to capture the substantive information exchanged and the interactions and behaviours involved.[6] In discussing how the Internet is actually used and how that usage may be impeded, the addition of this fifth nominal layer is helpful. The concept could be seen as very roughly analogous to the distinction in traditional telecommunications between network carriage and its content (although in the Internet’s case this is actually too binary a parallel for reasons that need not detain us). Accordingly, in this study we shall refer to a fifth “content and transactions” layer; the resulting scheme is depicted in Figure 1.

Figure 1: Internet Layers

5. Content and Transactions Layer
4. Application Layer
3. Transport Layer
2. Network/IP Layer
1. Physical/Link Layer

This sort of distinction between the underlying physical and software-enabled logical infrastructure and its utilization was central to the working definition of Internet governance that was agreed to by the United Nations Working Group on Internet Governance in 2005. Two of the authors of this paper were in that group and were centrally involved in developing the definition: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet."[7] By distinguishing between the infrastructure and the and its utilization and saying that governance occurs at both these broadly construed levels, the definition facilitated a clearer and ultimately more productive debate among governments and stakeholders in the World Summit on the Information Society (WSIS) and helped to shape the next decade of dialogue and action on global Internet governance.[8]

A closely related bit of nomenclature that was used at the time and has since taken its place in the lexicon was the distinction between governance "of" the Internet and governance "on" the Internet. This simple binary is actually a bit misleading and problematic insofar as processes and governance issues may extend across it. Moreover, it has lent itself to some unduly strategic discussions in which certain actors argued that e.g. rules and procedures pertaining to the "of" half of the binary are purely administrative and should be left out of discussions of "governance".[9] But as a simplifying heuristic device it also has proven useful in helping to ease discussions, so we adopt the convention here.

In the pages to follow, we discuss three forms of fragmentation:

- *Technical fragmentation: conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points.* These generally pertain to layers 1-4 of the model above.

- *Governmental fragmentation: Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources.* These generally are targeted at the 5th

layer in our model, but they may involve actions taken at the lower technical layers as well.

- *Commercial fragmentation: Business practices that constrain or prevent certain uses of the Internet to create, distribute or access information resources.* These generally are targeted at the 5th layer in our model, but they may involve actions taken at the lower technical layers as well.

We should note that some other observers refer to social or cultural forms of fragmentation. In this paper we do not treat the existence of different cultures, languages, social preferences, and so on as sources of fragmentation. They are simply sources of difference. They may be relevant if, for example, cultural sensibilities lead a government to undertake an action that is fragmentary, but we do not view them as independently causal of fragmentation. In addition, in addressing the roles of governments, we do not attempt to separately delve into what some call "legal fragmentation" due to the existence of different national legal systems.[10] The arguments for or against treating legal differences in this manner are best left to those in the legal profession.

Again, ours are working definitions proposed to facilitate discussion, and they may be fine-tuned or thoroughly rethought as the emerging dialogue on fragmentation unfolds. But for now they seem to approximately meet some key criteria for such definitions. These include: adequacy, or being "good enough' to capture the main meanings that seem to be in play when people discuss fragmentation; generalizability, or applicability across a broad range of current and potential conditions; conciseness, in that they do not appear to include nonessential terminological verbiage; and neutrality, in that they are not intrinsically normative.

It should be emphasized that while in the pages to follow we discuss the three types sequentially on a stand-alone basis, this is a convenience intended to reduce narrative complexity. In many cases, the driving considerations at work pertain to the content accessed and transactions undertaken by users, rather than by a desire to alter the infrastructure per se. For example, governments typically are focused on what happens at the top 5th layer of content and transactions rather than on how the lower layers operate. Even so, the pursuit of remedies to perceived problems in Internet usage often does lead them to take actions that directly or indirectly impact the underlying infrastructure. In some cases, the same may be said of commercial fragmentation. Here as elsewhere, the nominal boundary between fragmentation "of" and fragmentation "on" the Internet can be blurred.

The Variability of Fragmentation

As our trichotomy of technical, governmental and commercial fragmentation indicates, fragmentation is not singular in its sources or forms. But the

complexity of the matter does not end there. Within and across the three categories there can be a great deal of variation in its character. Indeed, one could devise a long list of attributes according to which any given instance of fragmentation may vary. To make the discussion more manageable, we highlight just four dimensions of variation that are applicable to our categories and the universe of examples we present in subsequent sections of the paper.

Occurrence

The first and most fundamental consideration is whether a given form of fragmentation exists. This is not an entirely straightforward question; fragmentation is not always a simple binary condition that is either present or not present. There can be gradations with different values along a continuum. In some cases those values can be precisely quantified (e.g. the number of websites or other information resources to which access is fully blocked), but in others the best we can do is to devise ordinal measures.

Similarly, there can be variations in duration. Fragmentation may be a short-term phenomenon that is rectified fairly quickly, as with recovery from some disabling cyberattacks, or it can be sustained as a long-term condition. In time sensitive situations, even short-term fragmentation can be very damaging to users or transactions. In general though, presumably we should be most concerned with sustained fragmentation with recursive consequences.

A final issue here is that fragmentation does not need to be currently present to be of concern. That is, in many of the instances that people cite when worrying about the matter and that we discuss in the sections to follow, what is at stake is the emergence of tendencies and pressures that could give rise to something significant in the future. As in any policy arena, we need not wait for a problem to become full blown and wreaking havoc for awareness and action to be well advised.

Intentionality

Fragmentation may be the unintended by-product of decisions and actions guided by unrelated objectives. A number of instances of technical fragmentation are of this character. People who deploy or fail to deploy a particular technology in addressing a localized operational challenge may not be setting out to fragment the Internet. Nevertheless, their actions, especially if replicated by others, could come to have broader effects. Divergences between individually rational choices and systemically suboptimal consequences are a standard feature of collective actions problems generally and the same logic can apply to the openness or fragmentation of the Internet.

Alternatively, fragmentation may be intentional. The character of these intentions obviously matters quite a bit. On the one hand, organizations, communities and individuals may seek to separate themselves somewhat from the open public Internet for entirely defensible reasons. Installing a firewall to limit access and communication to only authorized and consenting parties and to protect resources from unwanted interference is a benign act of self-separation. On the other hand, actors such as some governments may seek to shape, constrain or fully block the activity of others who have not consented to this. Imposing limitations on others is a malign act of forced separation. Both unintentional and intentional fragmentation can be problematic, but the best approach to remediation may vary accordingly. In some cases awareness raising, dialogue and coordination may be sufficient, but in others negotiations and even the application of pressure may be called for.

Impact

Fragmentation may be deep, structural and configurative of large swaths of activity or even the Internet as a whole. Consider, for example, the implications if significant categories of data flows were to be widely blocked around the world, or if an alternative root system with its own address and name space were to be established with the backing of powerful governments or organizations. The scope of the processes, transactions and actors impacted by such breakage would be substantial. But fragmentation also can be more shallow, malleable and applicable to a narrowly bounded set of processes, transactions and actors. The impact could be significant for some people but go unnoticed by others.

As with the other dimensions just mentioned, it can be difficult to measure the intensity of fragmentation and say with certainty exactly where on the continuum a given instance lays. Even so, in considering examples, we should be mindful that fragmentations are not all created equal in terms of magnitude and import. Indeed, a number of the examples we discuss are relatively low-impact or low-intensity matters – bothersome and concerning enough to engineers and operators that attention to them is merited, but not so significant that they endanger the fundamental integrity, openness and utility of the Internet. In contrast, some other examples we cover are higher-impact and arguably in need of concerted responses.

Character

Finally, irrespective of the strength of impact, duration, and so on, fragmentation also can vary along a continuum of, for lack of better words, “good” to “bad”. This is an admittedly squishy and difficult to measure attribute, but it captures something important because the tenor of the debate could easily lead one to believe that fragmentation is always and everywhere a bad thing. But of course, organizations, communities and individuals choose

all the time not to be perfectly reachable from all other end points. The widespread prevalence of firewalls, encryption and other security and privacy tools that allow users to carefully mediate their boundaries and decide which data they welcome to flow across these indicates that fragmentation also can be benevolent and valued.

Of course, whether something is viewed as good or bad can depend on norms and value judgments; a human rights defender may regard the dark web as a relatively safe place to communicate and thus a good sort of fragmentation, while a law enforcement or intelligence person may regard it differently.

Indeed, people can even have different views about whether significant, structural fragmentation is necessarily a bad thing. Most notably, Columbia University economist Eli Noam has elicited much debate with a short but suggestive broadside against those who argue that fragmentation is inherently bad; see the selection in Box 2.

Box 2: A Contrarian View

Instead of mourning about the passing of uniformity, we should embrace the emergence of diversity. We must get used to the idea that the standardized Internet is the past but not the future. And that the future is a federated Internet, not a uniform one. I used to think that this was regrettable but unavoidable. Even that upsets many people: how can one doubt the integrity of the one Internet that has served us so well? Now, I want to go one step further to argue that it is not regrettable at all. It is actually a good thing. The single Internet was a good system in the past but not in the future ….

A technical centrifugalism is inevitable. It is especially inevitable if it becomes readily possible to interoperate among different Internet flavours. To provide such interoperability across non-uniform protocols are intermediaries that supply 'bridging as a service'. These intermediaries are likely to be some of the emerging cloud computing providers … Most will be private, but some will be public and governmental. The ITU [International Telecommunication Union], too, could initiate such a cloud ….

The emergence of such a system of interconnected private Internet arrangements does not negate a public Internet. On the contrary, the two arrangements supplement each other. If private Internet arrangements are too restrictive, costly or discriminatory, the public system provides a safety valve, and vice versa. This will prevent such a system from becoming a walled garden of walled gardens, which would be unacceptable.[11]

This is, to be sure, a controversial view. But it raises a range of interesting questions about the overall evolution of the Internet as it becomes ever more ubiquitous and embedded in complex and diverse social orders; under what conditions might which forms of fragmentation be benevolent or pernicious; whether fragmentation is sometimes an inevitability to be managed and adapted to as best we can or is instead always a function of short-sighted decisions that should be questioned and remediated; and so on.

Conclusion

In this section we have sketched out our general analytical orientation to the problem of Internet fragmentation and proposed for working purposes three basic definitions that cover the universe of current and potential cases we have considered. In the next three sections we map out that universe.

2. Technical Fragmentation

When the Internet concept was first articulated, a guiding vision was that every device on the Internet should be able to exchange packets with any other device. Universal connectivity was assumed to be a primary benefit. One could not know when such connectivity might prove useful and to exclude any seemed self-defeating. It was further assumed, however, that no device could or should be compelled to engage in communication and that a recipient of a packet could reject or ignore it or impose certain requirements on any further communication.

There are a variety of ways in which the original concept of a fully connected Internet has been eroded over the course of the Internet's over 30 years of operation. Technical fragmentation of the underlying physical and logical infrastructure is a complex evolutionary process that has unfolded slowly but is gathering pockets of steam in the contemporary era. Some of it has been intentional and motivated by operational and other concerns, and some of it has been the unintended by-product of actions taken with other objective in mind. Moreover, the means by which such fragmentation has been achieved also varies in technical terms. To capture these realities, in this section we survey some key trends with respect to addressing, interconnection, naming and security in the Internet.

Addressing

The original design of the Internet used 32 bit numerical identifiers, analogous to telephone numbers, to designate end points on the Internet. Unlike the telephone numbering plan, however, IP addresses were not nationally-based. Their structure was related to the way in which the networks of the Internet were connected. Each network was made up of a collection of IP addresses associated with an autonomous system number. An endpoint on a given autonomous system or network could be anywhere on the globe, but endpoints of a particular autonomous system are all interconnected through that network.

The IP suite went through four major design iterations and the final form for the IP addressing was called IPv4. The 32 bit addresses were represented as four decimal values separated by periods such as 27.2.18.155. Each field has a value ranging from 0 to 255 (i.e. values that can be expressed in eight binary bits). This address format allowed for up to 4.3 billion possible terminations on the Internet. This so-called dotted notation does not reflect any hierarchical structure – it is merely a convenient way to express a 32 bit number.

Coordination of the numbering system is one of the Internet Assigned Numbers Authority (IANA) functions. The Internet Corporation for Assigned Names and Numbers (ICANN) currently performs the IANA functions, on

behalf of the US government, through a contract with the National Telecommunications and Information Administration.[12] ICANN allocates blocks of numbers to the five Regional Internet Registries (RIRs), which are non-profit corporations that administer and register the IP address space numbers within their regions.[13] The global multistakeholder community is currently hard at work on a plan to transition the US government's stewardship of the IANA functions to a newly independent and accountable ICANN, hopefully in 2016.

As the Internet was deployed commercially, it became apparent that there might not be enough numbers to serve all the possible terminations on the growing Internet. This realization triggered two developments. The first was the creation of private numbering plans that allowed for local use of IP addresses that could not be routed through the public Internet. Three distinct private address spaces allowed for networks of up to 256 devices, 32,384 and 16 million devices respectively. In order to allow local devices to communicate with other devices on the public Internet, these private addresses have to be translated into addresses that are routable in the public Internet. This is the second development associated with IP address limitations.

The process is called Network Address Translation (NAT) and it has become widely used to allow many local devices to share a single, public IP address. There is economic incentive for Internet service providers (ISPs) to implement this mechanism so as to maximize the number of subscribers whose devices can be serviced. This process introduces the possibility of a kind of fragmentation in the Internet because the *private addresses are isolated from the rest of the Internet unless they pass through a so-called NAT box* (that could be part of a router). In some cases, this isolation may, in fact, be an attractive feature of the NAT mechanism, in addition to the fact that a subscriber who is using private IP addresses does not have to renumber all his or her devices when changing to a new ISP since the NAT process takes care of the mapping into publicly routable addresses when needed.

Recognizing the potential depletion of the IPv4 address space, the Internet Engineering Task Force (IETF) that develops international standards for the Internet introduced a new address format called IPv6. This packet format allows for a 128 bit address space, sufficient to label 340 trillion trillion trillion endpoints in the public Internet. The expansion of address space comes with a price, however, because *the two formats, IPv4 and IPv6, are not compatible. It is necessary to run the IPs in parallel in what is called dual-stack mode.*

At present, only about 4% of the Internet is servicing IPv6 usage. There have been signs of late of growing momentum in IPv6 adoption, but clearly there is still a long way to go.[14] To make matters worse, most of the RIRs that assign IP address space to ISPs and other end users have essentially exhausted their supplies of IPv4 addresses and have only IPv6 address space to assign.

A market for IPv4 address space has developed but this can only postpone the inevitable need for more addresses. Even the use of NAT will not really prove adequate to serve the enormous anticipated needs of the Internet of Things. In addition, new computer chipsets and cloud computing environments allow for many virtual machines to operate on a single chip, leading to the need for multiple addresses to distinguish among the virtual systems.

The fragmentation risk is that the transition to IPv6 will continue to lag and result in IPv4 and IPv6 Internets that do not interwork. ISPs are being encouraged to implement both IPv4 and IPv6 services and end device makers are being encouraged to implement dual-stack IPv4 and IPv6. It *remains to be seen whether these remedies will keep the Internet fully connected,* with IPv6 being the eventual address format of choice in the longer term.

There are other special addresses ranges for multicasting, that is, sending packets to more than one recipient at a time. One variation on this is the so-called Anycast mechanism that allows computers in many physical locations in the Internet to receive traffic destined for a particular address and respond to it. This is in use in the Domain Name System (DNS), discussed below.

Interconnecting the Network of Networks

The routing of traffic in the Internet is accomplished by means of routing protocols used by routers to share information about the topology of the connections among the myriad networks that make up the Internet. An autonomous system is a set of networks and routers that form a connected whole. The Internet is made up of many such autonomous systems. The routers of any particular system use one of several possible interior gateway protocols to establish the connectivity of the system. Each router within an autonomous system maintains a table of information that allows it to determine the next hop for a packet in a path through the routers of the system until it reaches its destination in that system or arrives at what is called a border router or gateway to the next autonomous system along the packet's path to the ultimate destination.

The topology of the global network of autonomous systems (i.e. the Internet) is maintained through the Border Gateway Protocol (BGP) that allows the ensemble of border routers to determine how to route packets. There is a good deal of trust involved in this system and it is possible to inject false information into the routing system to cause packets to flow along paths not expected by the originator. Each autonomous system's border routers announce the Internet addresses that can be reached within that system and the BGP protocol allows all the border routers to form a global routing table. Although a good deal of attention is paid by the operators of the networks of the Internet to the possibility that false or incorrect information may be

inserted into the global routing table, *it is still technically possible for deliberate or accidental corruption of the routing data to occur.* Traffic can be routed into so-called black holes, for example, or along paths that allow surveillance. Technical means have been proposed to defend against such occurrences but they have not yet matured into use.

The operators of networks of the Internet determine on their own with which other networks they will interconnect and on what terms and conditions. There are several forms of interconnection. One form is called peering, in which a pair of networks connect directly with each other or through an Internet Exchange Point (IXP). It is typical that network peering is settlement free in the sense that the parties do not charge each other for carrying traffic, having concluded that they are receiving comparable value as a consequence of the mutual carriage. In a peering relationship, each ISP carries the other's traffic but only to subscribers of the carrying ISP, not to the ISP's other peers.

There is a second alternative connection method called transit in which one network pays the other to carry its traffic into the rest of the Internet. This is a typical outcome when a smaller ISP chooses to pay for service to all points of the Internet rather than building additional resources to establish sufficient peering connections to reach all of the Internet. The transit ISP delivers the received traffic to its customers and to all its peers. In practice, many ISPs make use of both methods. There is also a hybrid form of interconnection called paid peering in which the operators agree to carry each other's traffic to their respective customers but one ISP pays the other.

To date the system of private interconnection contracts among ISPs has ensured the provision of an integrated global public Internet. It is important to ensure that this is preserved even if the incentives to some operators begin to change in ways that could lead to increased costs and fragmentation; we return to this question in Section 4 of this paper.

As the Internet became a commercial service and was adopted by the private sector, legitimate interest in protecting computing assets from access by the "outside world" led to the design and implementation of firewalls that could filter traffic at the packet level. Certain protocols could be blocked, port numbers filtered, and even certain source or destination IP address ranges might be allowed or disallowed. This kind of filtering can be implemented in routers and in edge devices including personal computers. As the Internet of Things (IoT) becomes more prominent, considerable attention may be paid to white listing and strong authentication to protect devices, their controls and their information from unauthorized access.

Experience with firewalls has shown them to be insufficient for protection. One can physically walk past a firewall, bringing an infected laptop or memory stick into an enterprise and spread viruses and worms among the computers that are part of the internal enterprise network. *Firewalls are, however, a*

useful complement to other methods of protection. It seems fair to say that this is a positive form of fragmentation intended to protect enterprise or personal resources from unwanted connections.

The IPs allow for a virtual private network (VPN) service in which an ISP allows a customer to tunnel through its part of the Internet to a destination network. The VPN customer receives an IP address that makes it look as if it is part of the destination network connected through a typically encrypted tunnel through a part of the public Internet. *Users of VPNs isolate themselves from the global Internet and behave as if they are part of the target network.* Corporations with private networks connected to the Internet often use VPN tunnelling to support their employees who need to access corporate assets without exposing these to connection by general users of the Internet. *It might be argued that this capability represents a form of fragmentation. What is perhaps more of concern is that some national jurisdictions are blocking the use of the VPN protocols to prevent users from protecting their traffic from surveillance.* In actual fact, VPNs are losing some favour since a compromised laptop or desktop computer with a VPN connection to a corporate network may become the avenue for reaching the assets of the corporate network. Other means of end/end encryption and authentication are gaining favour.

In a variation on the VPN, there is the so-called TOR network or “onion space” that allows users to route traffic randomly through a network of forwarding nodes partly to obscure the originator of the traffic and to obscure the intended destination of the traffic to surveillance until it reaches its last hop. Typically, the traffic is encrypted for privacy until it reaches its destination. Ironically, TOR was originally developed by the US Naval Research Laboratory for use by the intelligence community for exfiltration of information and was later made openly available. It is widely employed by human rights activists and others with legitimate reasons to avoid government surveillance. But it also is the home *of a “dark web” of illegal activities* and thus poses challenges to law enforcement and intelligence operations.[15] This well illustrates the double-edged sword of the technologies of the Internet.

The Domain Name System

For flexibility, the protocols above the TCP/IP layer make use of domain names rather than numerical IP addresses to refer to sources and sinks of Internet traffic. Example.com is a domain name whose top-level domain is “com” and whose second-level domain is “example”. Domain names are essentially synonymous with the notion of a logical end point on the Internet: a client, server or edge computing device of some kind. Before higher-level protocols can make use of the lower-level protocols such as TCP or UDP, they must use the DNS to translate from the domain name form to a numerical IP address form. These applications perform a domain name

lookup using a system of resolvers and name servers that form the hierarchical DNS.

The top-level information of the DNS is called the root zone and it points to the name servers for the top-level domains (TLDs) of the Internet, of which there are now on the order of 1,200. They include the familiar ".com", ".net" and ".org" and country codes such as ".us", ".fr" and ".jp" and now hundreds of new top-level domains including ".restaurant", ".pharmacy" and ".capetown".[16] In addition to being easier to remember, domain names have the property that then can be translated into one or more IP addresses, and those addresses can be changed without changing the domain name. This means that persistent references can be made to a destination domain name even if the IP address of the destination in the Internet changes. If a website chooses to locate a server at a new IP address, it does not have to change its domain name. Rather, the name server for that domain name only has to respond with a new IP address when the name lookup occurs.

Originally there were only 13 root servers on the Internet that pointed to the TLD name servers but since that time, using the Anycast routing system, hundreds of root servers populate the Internet today.

In the beginning, domain names were expressed in Latin characters, letters A-Z, digits 0-9 and the hyphen. Upper and lower case was ignored for purposes of looking up domain names and translating them into IP addresses. As the Internet expansion continued, it was recognized that a broader range of scripts were needed to allow expression of domain names in Cyrillic, Greek, Chinese, Korean, Hebrew, Hindi, Urdu and many other languages. The IETF developed new standards for incorporating the Unicode character set into the DNS so that domain names could be expressed in many different scripts. *Internationalized Domain Names (IDNs) could lead to some forms of fragmentation, depending on how uniformly the processing of domain names is done across the Internet.* Depending on the software used, there can be variations and failures to successfully look up domain names in the so-called IDN format. Efforts continue to implement this processing in a uniform fashion to minimize unintended fragmentation of the system.

In its original formulation circa 1984, the DNS used a handful of generic top-level domain names (gTLD): .com, .net, .org, .edu, .gov, .mil and .int. A special TLD included .arpa to assist in a transition from the original ARPANET naming scheme to the DNS. Subsequently, two-letter codes created by the United Nations Statistics organization for countries and areas of economic interest were adopted as country code top-level domain names (ccTLD). There were on the order of 200 such codes, such as .us, .fr, .tk, .jp, .za, .ar (United States, France, Turkey, Japan, South Africa and Argentina, respectively).

ICANN added additional gTLDs between 2000 and 2011, and in 2012 launched the new gTLD Programme. In the first round of the programme it received 1,930 applications, and as of December 2015, it had approved and delegated 853 of these into the root zone file. Another 480 applications are proceeding through the process, 560 have been withdrawn, and 37 have not been approved or are otherwise not proceeding.[17] The expansion of the TLD space provides a broad range of choices for users to register second-level domain names such as abc.xyz and opens up many new opportunities for commerce, speech and community building. But it does raise an exceptionally wide range of issues that stakeholders and governments have laboured intensively to sort out, and among these involve new possibilities for fragmentation.

A commonly heard criticism of the program that is sometimes framed in these terms has been that proliferation will lead to user uncertainty as to which domain names are authoritatively associated with which organizations or company brands. It also raises questions about in which TLDs a corporation should register to avoid such confusion. To make matters more complex, trademarks can belong to more than one organization while domain names must be unique. Which Berlin is associated with .berlin? Is apple.com the same company as apple.coop? Users may end up at destinations that are not the ones they are expecting. Together with the spread of IDNs, this may increase the likelihood that users will rely on search engines rather than names to find the resources they seek, as well as the importance of finding ways to validate destinations. Probably people may disagree as to whether all this counts as a sort of experiential fragmentation or simply confusion amidst complexity.

More clearly a matter of fragmentation is that *there is a possibility that the proliferation of new gTLDs will lead to increased blocking within the DNS.* Already in 2011, many governments greeted ICANN's approval of the .xxx gTLD for pornography with announcements that they would simply block the entire domain. As more character strings are entered into the root zone file that some governments deem to be risky, sensitive, or contrary to their laws, more national blocking could ensue. Indeed, during the debates leading to the launch of the New gTLD Program, some governments and others argued for simply refusing approval to (some observers said censoring) certain strings on the grounds that widespread blocking was contrary to an open Internet and could even be technically destabilizing.

The technical community generally has disagreed with the latter argument, although at least some eyebrows were raised in October 2015 by VeriSign's quarterly filing with the US Securities and Exchange Commission. The company noted that, "In view of our role as the Root Zone Maintainer, and as a root server operator, we face increased risks should ICANN's delegation of these new gTLDs, which represent unprecedented changes to the root zone in volume and frequency, cause security and stability problems within the

DNS and/or for parties who rely on the DNS. Such risks include potential instability of the DNS including *potential fragmentation of the DNS* should ICANN's delegations create sufficient instability, and potential claims based on our role in the root zone provisioning and delegation process."[18] This legal prudence notwithstanding, it is unclear that instability will ensue, but *there may be more gTLD blocking and hence more fragmentation in the DNS.*

Another concern relates to the interfaces and possible collisions between public and private names. The DNS design was intended to respond with the same information no matter where the lookup originated. This is an important uniformity principal that is worth preserving to achieve a level of uniformity in the behaviour of the global Internet. This principal has already been altered by the *use of internal corporate name servers that resolve to addresses, e.g. inside a corporate network and which are not reachable from outside a corporate boundary. This is sometimes referred to as split-horizon DNS* and is useful for protecting access of corporate resources from outside the corporation network. There are also cases in which a lookup produces different results depending on the source IP address of the lookup. For example, looking up Google.com may actually resolve to the IP address of Google.fr or Google.za depending on the source IP address of the DNS lookup. More generally, "What was a relatively uniform common public space is now being fenced into a number of realms, many of which are private."[19]

There is another form of fragmentation that arises in the context paid access to Wi-Fe services in hotels, restaurants, etc. The user wishing to use the Wi-Fi service typically tries to open a web page somewhere on the Internet. The DNS lookup that follows is intercepted by the local router/resolver and a false response is returned that takes the user to a website that requests the user to log in or at least make a payment before access to the Internet will be permitted. For all practical purposes, the mechanics of this are like hijacking arbitrary domain names. One solution to this problem is the development of a protocol specific to the authorization and validation process for access to the local service rather than coercing the DNS lookup.

Preservation of a common root zone and common TLD space across the Internet has been an important unifying principal. Assuring that the information returned from a DNS lookup has been a high priority for protocol development and a method for achieving this uses digital signatures to bind the domain name to its associated IP address(es). The so-called domain name system security extensions (DNSSEC) standard is designed to allow the responses to domain name lookups to be checked for integrity and rejected if digital signatures do not match the expectations of the party doing the lookup.

DNSSEC is already in use in the Internet and, in particular, the root zone with its references to all top-level domains is being signed for integrity. This could allow any domain name resolver to cache a copy of the root zone and be

assured that the data has not been altered, and to reduce dependence on the existing system of Anycast root servers. We return below to DNSSEC and the use of cryptography.

There is nothing in the Internet design that inhibits the creation of alternative ways to map identifiers into IP addresses. There have been experimental attempts to create alternate roots so as to allow users to choose different mappings of domain names to IP addresses or new identifiers spaces to be mapped into IP addresses. These generally have not succeeded, in part because they either required browser plug-ins to get to the right server or changes in the recursive resolvers to achieve the same objective. *Alternate domain name roots create a prima facie hazard since the same names may map to different IP addresses and thus different servers. Users may land on a server that is only pretending to be the legitimate destination.*

A variation of this hazard has arisen in a current project called YETI that plans to import the root zone of the DNS that is managed by ICANN, strip the digital signature from the zone and re-sign with a YETI key.[20] *While its proponents assert that it is not intended to provide an alternate root, it does, in effect, do exactly that.* Once in place, it is possible for local resolvers to be configured to refer to the YETI name server rather than to the ICANN servers and all entries in the YETI root zone would appear to be valid if the YETI signing key is accepted. Although its ostensible purpose is to explore limits to root server performance and functionality, it has to potential to introduce an alternate root.

More generally, if ever leading governments or intergovernmental organizations were to implement an alternate root – a possibility that was sometimes raised in the highly charged geopolitical context of the WSIS negotiations – the results could be a game changer. *Indeed, the establishment of an alternate root that has significant government backing arguably would be the mother of all fragmentations.*

There have been other identifier spaces developed that map into IP addresses such as the Digital Object Architecture developed by the Corporation for National Research Initiatives.[21] Digital objects such as books, movies, music and other digitized content are assigned a unique and permanent identifier that can be looked up and mapped to an IP address where the object may be found. The importance of this work lies in the permanence of the identifier space. In the DNS, if domain name registrations are not renews, the domain names may no longer resolve and references to digital objects (e.g. web pages) using these domain names may no longer resolve.

Security

For security and access control, it was thought in the original conception of the Internet that devices that wished to communicate only with known and authorized correspondents would make use of shared cryptographic keys as a means of validating legitimate correspondents. If the contents of received packets could be correctly decrypted, this was prima facie evidence that the sending party had legitimacy since the sharing of keys implied it. Of course, if a key has been obtained by stealth, bribery or cryptanalysis, this assumption would be incorrect. Although public key cryptography had been the subject of a spectacular 1976 IEEE article, at the time the early IPs were being defined in 1973-1978, this concept had not developed sufficiently for implementation to become part of the basic Internet security design.[22] Since that time, public key cryptography has come into its own and is an important element for implementing confidentiality and authenticity in Internet-based exchanges.

In fact, the notion of certificates and certificate authorities has evolved, using public key digital signatures, to allow correspondents to authenticate one another by confirming that a particular domain name, for example, is verifiably bound to a particular IP address or that a particular public key is verifiably associated with a particular domain name. The World Wide Web hypertext transfer protocol (HTTP) added a security feature to become HTTPS. Its use invoked an exchange resulting in a shared symmetric key for cryptography and could also involve certificated validation by either party of the other's identity.

A certificate authority can issue a certificate that typically associates a public cryptographic key with an identifier (e.g. a domain name). The certificate is signed with the private key of the certificate authority that matches the authority's known public key. The recipient of the certificate can check the signature using the public key of the certificate authority. If it trusts the certificate authority and its signature, then it can use the public key in the certificate to authenticate the site associated with key.

The IETF that develops technical standards for and implements the software and hardware mechanisms of the Internet develops various means to resist fragmentation. To prevent alteration of the DNS mapping of domain name to IP address, which would results in serious fragmentation, they have developed DNSSECs. In this system, the association of the domain name and its IP addresses is digitally signed in the records of the DNS. A signed lookup can be requested to assure that the information has not been undetectably altered since the holder of the domain name put it in place. DNSSEC reduces the risk of fragmentation by compromised domain name resolvers.[23] With regard to routing, there also is a proposal that is not yet widely adopted and still needs technical refinement to protect the information distributed by the BGP from being corrupted by false announcements.

Finally, the use of Certificate Authorities to authenticate the binding of domain names and public keys has been shown to be at risk either by penetration of a Certificate Authority by technical means leading to the production of false certificates or by corrupting a Certificate Authority to produce them. Assuming widespread use of DNSSEC in the DNS, a new proposal from the IETF called DANE would lodge public keys in the appropriate zone files of the DNS, limiting the ability for an abuser to produce corrupt certificates.

In general, there is a trend towards the use of end-to-end cryptography to increase confidentiality and integrity of information exchanged through the Internet and the use of certificates and digital signatures to authenticate actors and the information they exchange. For example, a new proposal for protecting the privacy of domain name lookups is under consideration that would encrypt the domain name lookup itself. These practices are essential if widespread surveillance, deep packet inspection and other sources of privacy erosion are to be reduced.

Conclusion

In this section we have highlighted 12 kinds of technical fragmentation:

1. Network Address Translation
2. IPv4 and IPv6 incompatibility and the dual-stack requirement
3. Routing corruption
4. Firewall protections
5. Virtual private network isolation and blocking
6. TOR “onion space” and the “dark web”
7. Internationalized Domain Name technical errors
8. Blocking of new gTLDs
9. Private name servers and the split-horizon DNS
10. Segmented Wi-Fi services in hotels, restaurants, etc.
11. Possibility of significant alternate DNS roots
12. Certificate authorities producing false certificates

3. Governmental Fragmentation

The most common imagery of "governmental fragmentation" is of the global public Internet being divided into so-called "Balkanized" or digitally bordered "national Internets".[24] Movement in the direction of national segmentation could entail, inter alia, establishing barriers that impede Internet technical functions, or block the flow of content and transactions over the infrastructure. Pressure and trends in this direction do exist. But so do counter-pressures and trends towards greater openness. Movement in this direction would give greater weight to global norms and values as embodied in international human rights law or trade agreements. The dialectical interaction of these forces of convergence and divergence varies across issues, space and time, so it can be difficult to judge where the pendulum may be at a given moment. But at least in some arenas, we clearly see more signs of fragmentation than we did just a few years ago.

In this section we survey instances of fragmentation of and especially on the Internet that result from government action. After some brief historical context, we consider six clusters of issues: content and censorship; e-commerce and trade; national security; privacy and data protection; data localization; and fragmentation as an overarching national strategy.

National Sovereignty and Cyberspace

How to balance the demands for national sovereignty with transnational cyberspace has been debated since the start of the global commercial use of the Internet in the early 1990s.[25] This was simply a new chapter in a long-running story; since at least 1850, governments had devised a range of national policies and international regimes for communications and information in which the promotion of sovereign control over their segments of cross-border networks and information flows was a core foundational principle.[26] Some governments and international organizations began to contemplate publicly whether there was a need for new governmental and intergovernmental mechanisms to strengthen the hands of sovereign states with respect to the Internet.

Others were in favour of industry self-regulation and a "light touch" approach by governments. Within the United States, the Federal Communications Commission had differentiated between different classes of telecommunications and information services and treated the Internet as an unregulated application. The common view was that, "Limited government intervention is a major reason why the Internet has grown so rapidly in the US. The federal government's efforts to avoid burdening the Internet with regulation should be looked upon as a major success and should be continued."[27] Hence, proposals were made for innovative forms of global multistakeholder governance or the market-friendly harmonization of national laws.

Moreover, an open, free and unfragmented Internet was seen as a universal value and enabler of economic growth and development worldwide. This was reflected, inter alia, in the “Global Information Infrastructure Initiative” that was proposed by US Vice-President Al Gore during the ITU’s World Conference on Telecommunication Development in Buenos Aires in 1995. The vision of a new borderless world, of a new economy and a new philosophy of industry self-regulation or at least public-private co-regulation became mainstream thinking in the 1990s, first in the United States and then across the industrialized world and beyond.

All this promoted a popular imagination that on the eve of the 21st century there were now two interlinked but different worlds. On the one hand, there was the real world with an old economy and traditional borders, limited natural resources and classical business models. Here there were borders regulated by sovereign states on the basis of national interests. On the other hand, there was the virtual world with a new economy, borderless cyberspace, unlimited virtual resources (IP addresses, domain names), resources that can be reused (digital content), and innovative business models in which quantity, distance and duration did not play a role anymore. This was the borderless space managed by a multistakeholder community on the basis of universal values.[28] Some analysts even speculated about the erosion of the international system of sovereign nation-states.

But the nation-state system did not disappear. The over 3 billion Internet users live not in cyberspace, but rather in physical spaces overseen by governments with varying legal systems and policies. All virtual communication is enabled via physical servers that are located in concrete places and have to operate under the jurisdictions of host countries. And as governments began to adjust and embed the Internet into frameworks of public authority, patterns of policy-making took hold in a significant number of countries that entailed fragmenting selected domains of cyberspace.

The 2002-2005 WSIS negotiations crystalized and clarified the emerging differences in preferences across countries. On Internet issues generally and Internet governance specifically, industrialized countries and some developing countries argued against top-down governmental controls and for preserving an open Internet subject to enabling rules. But many members of the Group of 77 and China, as well as Russia and some former Soviet Bloc states, pushed for greatly expanded government controls, to be realized inter alia by replacing the US government’s special role viz. ICANN and the Internet’s root with an intergovernmental agency. These views ultimately did not prevail, and the agreements reached by governments generally struck a balance that supported a decentralized, multistakeholder and open approach to Internet matters, most notably by creating the Internet Governance Forum (IGF). Moreover, in the years to follow, quite a few developing country governments,

including some leading players, evolved their positions in a more liberal and multistakeholder-friendly direction.

Nevertheless, the desire among others for more state-led approaches has remained a configurative force on the global stage, and this has translated into actions in specific issue areas that have had or could come to have fragmentary effects. Arguably, some actions proposed or undertaken by the industrialized democratic countries that have consistently championed an open and integral global public Internet at times have had fragmentary implications as well. The need for attention to these issues is thus universal.

Content and Censorship

As with the advent of previous communications technologies like print and radio, concerns about the substantive content of the information flowing across borders arose early in the globalization of the Internet in general and the web in particular. And once again, the contested interplay between the overarching principles of the free flow of information and national sovereignty would configure a good deal of the politics of Internet communications in the decades to follow. This tension was already embodied in the 1948 Universal Declaration of Human Rights, while Article 19 states that every individual has, "the right to seek, receive and impart information and ideas through any media and regardless of frontiers", Article 29 holds that "everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society ... These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations,"[29] which privilege the rights of the sovereign nation-states whose government make such determinations. Moreover, the ITU Constitution gives states the right to cut off, in accordance with their national laws, "any private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency".[30]

So governments have a certain leeway in determining what is inconsistent with the national security and public order of their respective societies. In Germany, propaganda with Nazi symbols is forbidden, but in the United States it is protected speech under the First Amendment to the US Constitution. A freedom fighter in the eyes of one government may be a terrorist in the eyes of another country. Discussions in assemblies like the UN Human Rights Council, the Council of Europe (COE), the UN General Assembly and the WSIS have demonstrated the difficulties of agreeing on a common understanding about how the rights enshrined in Article 19 are to be interpreted and guaranteed. A good deal of progress has been made in fleshing out the relevance and applicability of international human rights laws to the Internet, but in the meanwhile governments often have operationalized

sovereignty viz. the Internet in accordance with their national laws and preferences.

Accordingly, the range of national approaches taken towards content regulation and censorship has grown steadily over the years. Documenting the techniques used and their incidence worldwide is the focus of a substantial literature and many online activist campaigns and information repositories, the contents of which we need not summarize here.[31] But scholars associated with the Open Network Initiative have offered a handy summary overview by documenting the evolution of efforts to censor or otherwise control expression and access to information across three "generations", as follows.

The first generation of controls centred on filtering cross-border information flows, e.g. by continuously blocking servers, domain names, IP addresses, or keywords via filtering software or by inserting instructions into choke point routers at international gateways or among ISPs. Second-generation techniques expanded to include laws and regulations supplementing and legitimizing such technical measures by establishing notice and takedown requirements; lawful interception procedures; expansive cybersecurity requirements; the application of long-standing speech restrictions from the offline world pertaining to child abuse, slander, sedition, defamation and hate speech and to mass media veracity and objectivity; and the forced registration of websites, bloggers and users, or the revoking of ISP licences.

New types of technical interference sprouted up as well, sometimes provided by "rent a hacker" and other commercial operations. These could include network disconnections and resets; "just in time" event-oriented disruptions made to look like technical errors; distributed denial of service attacks launched by networks of compromised "zombie" computers; or DNS cache poisoning attacks that can cause a name server to return an incorrect IP address and divert traffic to an attacker's or other unintended computer. Finally, with contemporary third-generation controls, "The focus is less on denying access than successfully competing with potential threats through effective counter-information campaigns that overwhelm, discredit, or demoralize opponents. Third-generation controls also focus on the active use of surveillance and data mining as means to confuse and entrap opponents."[32]

Without delving deeper into this vast terrain, what matters here is that some of these approaches clearly introduce fragmentation. *Filtering and blocking; launching disruptive attacks with lasting effects on websites or other information resources; or denying access to social networks and applications used by millions and even billions of other users – actions like these fragment global public cyberspace.*

Often the damage done is restricted to particular user populations and swaths of content and experience, but sometimes there also are knock-on effects that ramify across the network of networks. While from a technical standpoint the Internet's overall security and stability have not been imperilled, the untrammelled proliferation of such practices, especially in combination with other sources of fragmentation, significantly detracts from the Internet's power as an engine of global development and empowerment. A human rights-centred analysis of these and other efforts to impede the exercise of internationally recognized rights such as freedom of expression and access to information would be an important addition to our understanding of fragmentation.

E-Commerce and Trade

When the globalization and commercialization of the Internet took off in the early 1990s, many governments were uncertain about its significance for economic growth and development and slow to adjust to the emerging realities. But today it is widely if not universally understood that networked commerce and trade are a key driver and growth pole of the world economy. Indeed, it is becoming commonplace today to speak of a shift to an "Internet economy", arguably with more justification than there was for some of the antecedent terms employed in earlier phases of the digital age like the "post-industrial" or "new" economy. How to measure its precise size and shape remains a vexing question with which economists continue to struggle.[33] But, for example, one widely noted estimate is that by 2016, the Internet economy will be worth $4.2 trillion in the G-20 countries alone.[34]

Given the economic stakes involved, governments everywhere are working to assess the opportunities and risks and to devise national digital strategies. This includes many governments in the Least Developed Countries. The evidence available in a variety of studies suggests a strong relationship between openness to the Internet and wealth creation.[35] Nevertheless, governments are often tempted to play for time and pursue approaches that preference national/regional players and digital spaces, including by restraining first-moving companies from abroad. In this context, the predominance of US technology companies in key market segments has led some governments to consider or adopt laws and regulatory practices that hinder certain kinds of operations and transactions or block the use of particular tools, be it social networking platforms or cross-border delivery via 3D printing.

Such practices have fuelled concerns that we may be entering a new phase of digital protectionism.[36] This charge may be rejected by other actors who argue that governments are merely trying to cope with a range of unprecedented challenges to their national identities and independence, tax bases, citizens' rights, and so on. For example, in September 2015, 51 Members of the European Parliament issued a statement that they were

“surprised and concerned about the strong statements coming from US sources about regulatory and legislative proposals on the digital agenda for the EU. While many of these are still in very early stages, President Obama spoke of 'digital protectionism', and many in the private sector echo similar words … Artificially deepening the Transatlantic divide on digital topics is not what we need. Instead, let's build trust and exchange ideas, but accept that a variety of views are an integral part of our open democracies.”[37]

While such strains and tensions are a cause for concern, there are also signs of progress in opening markets on the Internet. At the multilateral level, the 15-19 December 2015 Ministerial Meeting of the World Trade Organization (WTO) agreed to maintain the current practice of not imposing customs duties on electronic transmissions until its next session in 2017, and to breathe new life into the conceptually and politically difficult Work Programme on Electronic Commerce.[38] In addition, participants in the Information Technology Agreement established a timetable for eliminating tariffs on a wide range of products of direct relevance to the vitality of the Internet economy.

At the plurilateral level, the Trans-Pacific Partnership (TPP) negotiations concluded on 5 October 2015 produced a text with strong liberalization commitments on telecommunications and electronic commerce. Among other things, the latter proscribes barriers to the cross-border transfer of information, as well as requirements that companies use or locate computing facilities in a member’s territory as a condition to do business there. Similarly, work continues on the Trade in Services Agreement and the Transatlantic Trade and Investment Partnership, and the Organization for Economic Cooperation and Development (OECD) is pursuing a substantial work program that includes a focus on preserving an open Internet. And at the regional level, the European Union (EU) is actively pursuing its multidimensional Digital Single Market initiative, while the African Union, the Association of Southeast Asian Nations and others are advancing their respective programs to promote digital trade.

In short, global electronic commerce and the Internet economy been normalized into the global trade policy arena, and as such are becoming subject to its characteristic tensions and countervailing trends. What does this mean for Internet fragmentation? This is at best a nascent conversation, but one can imagine at least two contending position. On the one hand, it could be argued that any barrier to trade over the Internet constitutes a prima facie example of fragmentation at the content and transactions layer. On the other hand, it also could be argued that some barriers do not completely block transactions, but rather just increase the cost and difficulty of doing business, i.e. the “e-friction” involved.[39] At a minimum, it seems clear that *digital protectionism that blocks users’ access to and use of key platforms and tools needed for electronic commerce constitutes fragmentation on the Internet.*

National Security

While the military and intelligence establishments of countries like the United States began to think about the interplay between the global Internet and national security in the 1990s, most governments did not really focus on the matter until the beginning of this century. The terrorist attacks on 11 September 2001 in the United States proved to be catalytic. At the national level, many governments took cues from the US Patriot Act legislation and began to elaborate policies, although there was no shared global understanding about the precise boundaries and conduct of national security protections.

At the international level, 9/11 helped to push the quick adoption of the COE's Budapest Convention on Cybercrime in October 2001. The agreement came into force in 2004 and now has more than 50 members. The convention is a binding treaty that sets standards for some aspects of national law regarding substantive criminal and procedural laws, and it promotes international cooperation and mutual legal assistance among states. It also set out a shared framework regarding cybercrime by introducing definitions of hacking and other unauthorized access to networks and computers, but did not directly address broader questions of national security such as the rules of "information warfare" between states or between states or with non-state attackers.

In the years to follow, the range and diversity of cyberattacks grew and further stimulated many governments to develop "national cybersecurity strategies".[40] The protection of critical infrastructures and other national assets against political and economic cyberespionage at times led to planning for both defensive and offensive operations. Many governments began to treat national security as a concept that included and justified the control of political communications and cross-border content more generally. The slippery slide down this slope has been gathering momentum ever since. The Arab Spring begun in 2010 offered a significant example of how the Internet can help people organize for political change. Accordingly, some governments concluded that there was a need for more control over Internet communications, and perhaps even the need to centralize connections to allow for the termination of all Internet connections at a single point, as several Arab countries had done. Legislation introduced in the US Senate in 2010 to require an "Internet kill switch" was not passed, but it helped to foster a line of thought within some governments.

All this deepened the above-mentioned trends towards the spread of restrictive national laws and practices to block online content and the use of social networks in countries like Turkey, Iran, China, Pakistan, Russia, the former Asian Soviet republics, and many others. In the name of strengthening national security, *more states built defensive "walls" of varying widths and heights around their territories and sought to channel Internet*

communications via a limited number of gateways that could be more easily controlled. The 2013 Snowden revelations strengthened the drive, and the mistrust by some governments was extended also to US companies that operate globally, from Facebook and Google to Amazon and Apple. Proposals were discussed for "no spying" agreements and data localization practices began to take shape, as is discussed below.

With regard to international instruments, in September 2011, China, Russia, Tajikistan and Uzbekistan submitted to the UN General Assembly a call for a voluntary International Code of Conduct for Information Security. The draft code called on states to cooperate, inter alia, to curb "the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment … reaffirm all the rights and responsibilities of States to protect … their information space and critical information infrastructure from threats, disturbance, attack and sabotage … [and] lead all elements of society, including its information and communication partnerships with the private sector, to understand their roles and responsibilities with regard to information security."[41] A revised text submitted in 2015 softened the language in hopes of garnering broader support, but the underlying desires remain evident in other actions and pronouncements by its proponents. In contrast, the BRICS countries (Brazil, Russia, India, China and South Africa) continue to discuss a legally binding instrument for cybersecurity, as was proposed during their 2014 summit meeting in Fortaleza.

In a similar spirit, in the summer of 2015, the Group of 77 and China submitted an input for the High Level Meeting to review progress on the WSIS agenda at the UN General Assembly held on 15-16 December 2015. The document argued that governments should "proscribe the use of the Internet for activities that are illegal, unlawful, and detrimental to the global law and order. Any pictures, videos, and messages that incite violence and/or promote terrorist activities should not be allowed to be circulated on the Internet."[42] In short, to promote national security, a number of governments are calling for *multilateral agreements under which they could police a potentially wide range of messages with full international political legitimacy.*

Other governments are proceeding more cautiously in keeping with the complexity of the emerging issues. Based in part on the ideas laid down in the 2014 Tallinn Manual, the NATO states are arguing for the use of the existing international treaties, such as the 1948 Geneva Conventions on Humanitarian Law, as the legal basis for military conflicts in cyberspace. The Group of Governmental Experts operating under the 1st Committee of the UN General Assembly is working towards a common understanding of cybersecurity, in particular in the military field. The first results of this effort include agreements on transparency in national cybersecurity strategies and a set of confidence building measures, such as a July 2015 agreement on intergovernmental

cooperation and communication in cases of cyberattacks. The September 2015 US-Chinese agreement to ban economic cyberespionage was an important step, and similar efforts are under way in the Organization for Security and Cooperation in Europe. The African Union adopted a Convention on Cyber Security and Personal Data Protection in July 2014.

The above concise summary of a huge area of activity points to three broad conclusions. First, *national policies that entail blocking and censoring the Internet, or centralizing points of international interconnection in order to allow for "kill switch"-type responses,* introduce fragmentation at different levels of the Internet. Second, *cyberattacks that damage foreign networks and key assets in ways that cannot be quickly repaired* may also cause fragmentation. And third, *international policy frameworks that provide international political legitimacy for restrictive responses* also could be supportive sources of Internet fragmentation.

Privacy and Data Protection

Prior to the Internet's take-off as a global platform for e-commerce in the 1990s, the blossoming of data communications and information services in private networks gave rise to concerns about what was happening within these transnational corporate cyberspaces. At a conference organized by the OECD in 1974, an expert group dubbed the phenomena ''transborder data flows'' (TDF), which in contrast to ''international'' data flows invoked a mental image of corporate activities unmediated by territorial boundaries and authority, and raised the question of whether it constituted a problem of sufficient importance to merit regulatory action.[43]

Privacy and data protection for the transfer of personally identifiable information transmitted across borders quickly emerged as driving concern in this debate. Of particular concern were the different levels of protection afforded by the omnibus legislation being adopted in many European countries and the more limited and issue-specific laws being adopted in the United States. To square the circle and find common ground that would help facilitate both data flows and a sufficient level of protection, in 1980 the OECD established nonbinding but useful Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which were revised for the Internet age in 2013. These set out basic principles, inter alia, on the collection, quality, usage and protection of personal data, as well as the rights of data subjects. Going further, in 1981, the COE adopted a related treaty instrument, the Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; in 1995, the EU established its Data Protection Directive, which is soon to be superseded by a General Data Protection Regulation; in 2000, EU and the United States agreed their Safe Harbor agreement to provide a streamlined way for US-based companies to satisfy the EU Directive's "adequacy" requirements through voluntary self-certification; in 2005, the Asia Pacific Economic Cooperation adopted a

Privacy Framework; and so on. These plurilateral and regional agreements went a long way towards ensuring the continuity of TDF, although of course many privacy advocates would prefer further progress on data protection.

Efforts to harmonize privacy and data protection on a broader multilateral basis are still in a very early stage. But in December 2014, the UN General Assembly agreed to establish the position of a special rapporteur for privacy under the UN Human Rights Council. The mandate of the rapporteur includes, inter alia, the analysis of national privacy and data protection legislation. Such reporting could help to identify issues for elaboration in any effort to devise a global framework.

These issues became more contentious following the 2013 revelations by Edward Snowden. On 6 October 2015, the European Court of Justice (ECJ) determined, inter alia, that the 2000 US-European Union “Safe Harbor” agreement is invalid; that the European Commission (EC) was not competent to restrict the powers of national data protection authorities; and that the Irish data protection authority is required to decide whether the transfer of data pertaining to Facebook’s European subscribers to the United States for processing should be suspended on the ground that that country does not afford an adequate level of protection of personal data. The decision has been heralded as a victory by privacy advocates and many civil libertarians, but has left companies and the US government scrambling to work out new arrangements to avoid service disruptions while meeting the privacy concerns. The EU issued supportive guidance on trans-Atlantic data transfers on 6 November 2015, and efforts to find solutions are advancing.

Finally, it should be noted that the Safe Harbor decision comes just one year after ECJ’s Right to be Forgotten ruling that allows individuals to apply to search providers to have hyperlinks removed from the search results based on their names on the grounds that these links are harmful and meet the criteria for being suppressed. In addition to the palpable tension between the individual’s new right of removal and the public’s right to access information, it is noteworthy that this ruling applies to search engine operators if they have a branch or a subsidiary in an EU member state even if the server processing the data is located abroad. To the extent that the ruling is used to remove links to information that remains in the public domain, one could argue that its implementation introduces a measure of fragmentation.

Not surprisingly, some advocates of unfettered TDF have questioned whether the motivation behind EU privacy policy is not digital protectionism and, even if it is not, whether the policy might not anyway be inadvertently employed to protectionist effects. This sort of talk has caused privacy advocates and European policy-makers to object that, as one scholar put it, “A review of the historical record concerning the evolution of data flow restrictions in EU data protection law indicates that they are based more on policy considerations,

such as avoiding circumvention of the law and guarding against specific data processing risks in other countries, than on protectionism."[44]

In general, the strains between advanced industrial democracies with respect to the scope and modalities of privacy and data protection are best seen in the light of differences in legitimate policy preferences and legal systems. They can increase the level of digital friction and costs involved in some business processes, but they generally have not blocked flows and actively caused fragmentation on the Internet. On the other hand, in the context of new data localization requirements (discussed next), *strict privacy rules that deter or prohibit data flows have been introduced by some governments that are not otherwise known to be privacy defenders.* Such privacy rules could be seen as having fragmentary effects.

Data Localization

As noted at the outset of this paper, the post-Snowden uptick in data localization proposals and policies has been a major driver in pushing fragmentation up the agendas of business and governments and into the mass media space. But as with Internet fragmentation more generally, "data localization" is a multidimensional construct. And here too, the scholarly and policy literatures on the matter are nascent and a bit thin. Discussions of the issue often draw principally on a few cases, which makes it a bit difficult to generalize and arrive at a completely satisfactory definition of the problem. But one observer has offered a broad yet seemingly sufficient definition, suggesting that localization be understood as comprising, "laws that limit the storage, movement, and/or processing of data to specific geographies and jurisdictions, or that limit the companies that can manage data based upon the company's nation of incorporation or principal sites of operations and management".[45]

This formulation encompasses five distinct types of territorially-based restrictions. First, there are *requirements that data be processed by entities located within a given jurisdiction.* Second there are *requirements that data be locally stored or "resident".* Third are *network architectures and routing changes that strongly encourage or require data to circulate largely or solely within a territorial space*. Examples here could include Deutsche Telekom's proposal to reroute data within Germany, or the seemingly now abandoned concept of a "Schengen Cloud". Fourth are *discriminatory policies that select the organizations that may perform any of these tasks based on their national origins.* And fifth *are restrictions on the transborder movement of certain categories of data*, e.g. requirements of prior consent, or outright bans. If one examines the scattered but important evidence of localization policies in place today, there is notable variability as to the precise mix from these five types of restrictions that is applied in any given country.

With the exception of the proposed routing schemes, these types of localization are not really new. Indeed it is probably the case that they are more widespread and long-standing in certain sectors and issue-areas than is commonly recognized. For example, there is anecdotal evidence that the operators of websites and services associated with certain government-run or parastatal national ccTLDs are obliged to use nationally-based servers and providers for data processing and storage. More generally, it seems probable that many governments have localization requirements pertaining to certain types of public sector information, especially with respect to national security matters. Even the United States has at times looked askance at certain foreign vendors seeking entry to markets deemed sensitive, sought to restrict the cross-border flow of encryption technologies, and most likely has some selective limitations on where government data is processed and stored. Such instances would seem ripe for investigation in the context of any “deep dive” assessment of localization practices.

These special cases aside, mainstream business processes previously have gotten a hard look and at times been the focus of local process/storage requirements and data flow limitations. During the above-mentioned TDF debate of the 1970s-1980s, an issued raise at the outset concerned possible vulnerabilities to disruption when relying on information held in foreign jurisdictions. An often-cited example concerned the Malmö fire department, which located all its data on local fire hazards and facilities in a General Electric computer in Ohio, rather than in Sweden. What would happen if the systems involved performed poorly or went down entirely amidst an emergency? Building out from such examples, many governments began to express concerns that their “information sovereignty” could be imperilled if important data was not processed and stored within their national boundaries. It did not take long for the overarching issue to be cast as “TDF vs national sovereignty”, or for a whole host of socio-cultural, legal, economic and political issues to be raised within this framing. Such expansive framings of sovereignty are today enjoying something of a come-back, as is discussed below.

Possible regulatory and other solutions were considered both in the OECD and the Intergovernmental Bureau of Informatics, a now defunct organization with over 40 members, mostly developing countries.[46] In parallel, some governments began to enact localization requirements and restrictions on TDF. A notable example was Brazil, which in 1976 required local processing and prior approval to transfer certain kinds of business data out of the country. But a number of other countries considered or took tentative steps to impose localization requirements and cross-border limitations as well.[47]

In the end, the argument prevailed that imposing data localization requirements and impeding data flows would do more harm than good. The calls from new multilateral regulations gave way to the adoption of regional and plurilateral instruments that effectively locked in a rough consensus

among the key players that corporate TDF should generally occur without governmental impediments. The incipient national restrictions were generally lifted or softened, the Intergovernmental Bureau of Informatics was shut down, and in 1985 the OECD adopted a broadly framed Declaration on Transborder Data Flows that invoked the need to ensure access to data held abroad but generally urged governments to avoid the creation of barriers and limitations.

Flash forward 30 years and many of the same arguments that were raised about data flows over private corporate networks are being revisited and augmented with respect to the Internet. Concerted efforts to enhance international dialogue and cooperation and the mobilization of domestic critics has reduced some of the pressure and led some governments to reconsider their initial reactions. Brazil again provides a key example, having removed a data localization requirement before passing its Marco Civil law in April 2014. Nevertheless, other countries have moved forward with a variety of plans, sometimes with the strong support of nationally-based companies and social constituencies that believe they will benefit from restrictions.

The Russian government has taken the most widely commented-on initiative. Effective 1 September 2015, ITS law requires companies to process and store data about Russian citizens on servers within the country. It is unclear just how consistently or aggressively the law will be applied. While there are reports of US-based multinational companies investing in new facilities in order to comply, there are also reports that key Internet firms have been able to work out arrangements or have otherwise been exempted from some requirements.[48] Either way, as the law is “the latest in a string of about 20 laws tightening government control of the Internet” since 2012, it would appear to be part of a comprehensive policy framework.[49]

China also has added data localization requirements to its longstanding comprehensive policy framework to the Internet. In 2013, personal data protection guidelines were adopted to regulate “all or part of the process of processing personal information through information systems”, and these are reported to apply “to all kinds of organizations and institutions other than the government agencies and other institutions which exercise public management responsibilities”. Among their provisions is that, “Absent express consent of the subject of the personal information, or explicit legal or regulatory permission, or absent the consent of the competent authorities, the administrator of personal information shall not transfer the personal information to any overseas receiver of personal information, including any individuals located overseas or any organizations and institutions registered overseas.”[50] While the guidelines are technically voluntary, it is reported that, “The government distributed a document to some American tech companies earlier this summer, in which it asked the companies to promise they would not harm China’s national security and would store Chinese user data within the country … The letter also asks the American companies to ensure their

products are ‘secure and controllable,’ a catchphrase that industry groups said could be used to force companies to build so-called back doors – which allow third-party access to systems – provide encryption keys or even hand over source code.”[51] In parallel, the Ministry of Public Security reportedly plans to set up “network security offices” staffed by police within major Internet companies.[52]

Other countries, including some industrialized democracies, have implemented data localization as piecemeal solution to specific issues. For example, Australia prohibits the export of personally identifiable health records; Switzerland requires the prior consent of data subjects before financial records can be transferred across borders; some Canadian provinces require that some government institutions store personal data domestically; South Korea is said to prohibit the storage of mapping data on servers outside the country; and so on. The policies being proposed or enacted by many governments of all political persuasion are diverse in substantive scope and technological modalities, but collectively they point to a more densely bordered operating environment for multinational firms.[53]

In some cases, there may be reasons to question the motivations involved. For example, as noted above, some of the governments involved engage in quite significant levels of digital surveillance of their populations, and applying data localization requirements may simply make their jobs easier. Localization is also unlikely to greatly affect the operations of foreign intelligence agencies. As one analyst summarizes, “The notion that data must be stored domestically to ensure that it remains secure and private is false. In regard to security, while certain laws may impose minimum security standards, the security of data does not depend on where it is stored, only on the measures used to store it securely.”[54] It may also be that multinational companies are more likely to effectively guard their customers’ data than some of the local alternatives.

Localization may not succeed as an economic strategy, either. For example, two observers have argued that it “raises costs for local businesses, reduces access to global services for consumers, hampers local start-ups, and interferes with the use of the latest technological advances … Data localization, like most protectionist measures, leads only to small gains for a few local enterprises and workers, while causing significant harms spread across the entire economy. The domestic benefits of data localization go to the few owners and employees of data centres and the few companies servicing these centres locally.”[55] In a similar vein, a group of economists reviewed recently proposed or enacted legislation in seven jurisdictions, and concluded that the negative impacts on GDP would in every case be substantial.[56] Unsurprisingly then, some advocates of open TDF and digital trade are arguing that it is time for the WTO to take an active role, e.g. by enforcing existing trade laws that may be of relevance, extending its dispute

settlement mechanism and establishing a comprehensive database to track localization measures worldwide.[57]

Data localization measures create high transaction and other costs across industry operations, require the reengineering of systems and services, and may not be in the best interests of national economies and citizens/end users. But what do they mean for the Internet itself? *Data localization in the form of domestic processing and residency requirements, and the blocking of certain data flows, introduces new forms of fragmentation on the Internet at the content and transactions levels.* Moreover, depending on how it was done, *localization in the form of changes to the Internet's routing arrangements could entail broader fragmentation.* It may be that Internet technical administrators and operators would find ways to work around such barriers, but the risks would not be negligible.

Cyber-Sovereignty

The negotiations leading up to the UN General Assembly's 15-16 December 2015 10-year review of the WSIS highlighted that there remain fundamentally different conceptions among states of Internet governance that have important potential implications for fragmentation. For example, in a summer 2015 input to the preparatory process, the Group of 77 and China invoked the centrality of sovereignty and territorial integrity with respect to surveillance; "Improving Internet governance should entail establishing a multilateral, democratic and transparent international Internet governance system that ensures participation of all Governments, reasonable allocation of Internet resources, and joint management of key Internet infrastructure;" and suggested that, "The outcome document should consider establishing an intergovernmental forum on enhanced cooperation," a term the coalition previously has interpreted to mean the creation of an intergovernmental body with broad global policy-making authority.[58]

In parallel, the Russia government's summer 2015 input offered the following draft declaratory provision: "We note the need to ensure security and resilience of the critical Internet infrastructure in order to prevent outside manipulation, and for this purpose we call upon States to implement the storage of personal data of their citizens inside the territory of their own countries, to place domestic servers serving national segments of the Internet and to develop other elements of the critical Internet infrastructure."[59] In fact, the need to establish a clearly demarcated "national Internet segment" subject to strong governmental oversight has been an increasingly consistent theme of Russian policy pronouncements at both the domestic and international levels in recent years.

After intensive negotiations, none of this language was included in the final WSIS+10 Review outcome document that was approved by the General Assembly. To the contrary, the approved text for the first time paired

multilateral cooperation with multistakeholder cooperation in a generally sound and balanced outcome. But the build up to the 15-16 December WSIS High-Level Meeting did demonstrate that 10 years after the WSIS negotiations, some governments still desire to enshrine and build out state sovereignty as an organizing premise of national and global Internet governance.

On 16-18 December 2015, the government of China convened its second annual World Internet Conference. President Xi Jinping gave a keynote speech indicating that the promotion of "cybersovereignty" was the foundational principle of the Chinese vision of Internet governance. The President averred that, "The principle of sovereign equality enshrined in the Charter of the United Nations is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace … We should respect the right of individual countries to independently choose their own path of cyber development and model of cyber regulation and participate in international cyberspace governance on an equal footing …The existing rules governing cyberspace hardly reflect the desires and interests of the majority of countries …There should be no unilateralism [in building an Internet governance system]. Decisions should not be made with one party calling the shots or only a few parties discussing among themselves."[60] Russian Prime Minister Dmitry Medvedev reportedly supported Xi Jinping's proposals in his own speech, indicating that China and Russia are acting in close partnership to promote this principle of governance.

The linked concepts of "national Internet segments" and "cybersovereignty" imply Internet that, like the traditional public switched telephone networks of the pre-market liberalization era, the Internet's technical architecture should be organized into a series of vertically segmented, stand-alone national domains with interconnecting international gateways to hand off traffic. Control of the architecture and its usage to constitute discrete cyberspaces of content and transactions could provide the basis for a wide range of fragmentation-inducing national policies that some governments are already pursuing, and if embraced elsewhere could encourage such policies' replication and extension into new arenas. Of course, it is possible that these schematic vision statements will not have the readily imaged fragmenting effects in implementation. But the actions taken of late with respect to data localization and other issues may suggest otherwise. Either way, dialogue and clarification of their operational meaning would be useful.

Concern about the possible strengthening and spread of these orientations has influenced Internet governance processes in arenas beyond the WSIS Review. For example, the current drive to transition stewardship of the IANA functions from the US government to ICANN and its multistakeholder community has been lent added urgency by fears that any failure could encourage discontented governments to contemplate more fragmenting

actions, in the worst case scenario including backing a separate root. Hence, as Fadi Chehadé, the outgoing ICANN President and CEO has put it, “If we cannot find a way to govern the Internet on an equal footing, in an open transparent way this year, we might descend into a fragmented version of the Internet …The moment we fragment the Internet it is possible there will be tariffs between borders, there will be rules ... it will not be the Internet as we know it.”[61]

Other global multistakeholder collaborations also have been working to promote an open and unfragmented Internet. Participants in the 2014 NETmundial meeting in São Paulo adopted a set of principles and a roadmap for future collaboration in Internet governance that was decidedly of this character. Indeed, one of the overarching principles agreed to in the NETmundial Multistakeholder Statement was that the “Internet should continue to be a globally coherent, interconnected, stable, unfragmented, scalable and accessible network-of-networks, based on a common set of unique identifiers and that allows data packets/information to flow freely end-to-end regardless of the lawful content.”[62] The annual IGF meetings too have devoted significant time over the past decade to exploring the themes of Internet openness and access, and have featured sessions concerned with Internet fragmentation. And “native” Internet bodies like the IETF, the RIRs and the Internet Society are all pursuing work programs promoting a stable, open and unfragmented Internet.

In sum, we still have two competing, broad-based visions at work with respect to the role of governments and the character of public policy with respect to the Internet. It is unclear how their interplay will influence the prevalence of Internet fragmentation in the years ahead, but it is seems reasonable to assume that even if some governments opt anew for a vision of open networks, communications and markets, others who rule a significant share of the global Internet’s user population could be moving in other directions that expand the scope of government-induced Internet fragmentation.

For now, some close observers are extrapolating from the current signs and arriving at dark visions of the future. For example, Eugene Kaspersky argues that, “What may prove to be the ultimate game-changer is the fragmentation of the Internet…If the trend spreads, which is likely, such fragmentation will bring about the creation of parallel networks as governments the world over try to isolate their critically important communications. Such networks with no physical connection to the Internet are already widely used for military communications. Internet fragmentation will bring about a paradoxical de-globalization of the world, as communications within national borders among governmental bodies and large national companies become increasingly localized … As a result, the whole notion of netizens, or global online citizens, and of the Internet being a global village could lose all practical meaning. What could emerge is a patchwork of online nation states with different rules

and regulations and hindered communications."[63] Avoiding such a future will require vigilance, dialogue and cooperation.

Conclusion

In this section we have highlighted 10 examples of governmentally-induced fragmentation:

1. Filtering and blocking websites, social networks or other resources offering undesired contents
2. Attacks on information resources offering undesired contents
3. Digital protectionism blocking users' access to and use of key platforms and tools for electronic commerce
4. Centralizing and terminating international interconnection
5. Attacks on national networks and key assets
6. Local data processing and/or retention requirements
7. Architectural or routing changes to keep data flows within a territory
8. Prohibitions on the transborder movement of certain categories of data
9. Strategies for "national Internet segments" or expansive "cybersovereignty"
10. International frameworks intended to legitimize restrictive practices

4. Commercial Fragmentation

A variety of critics have charged that certain commercial practices by technology companies also may contribute to Internet fragmentation. The nature of the alleged fragmentation often pertains to the organization of specific markets and digital spaces and the experiences of users that choose to participate in them, but sometimes it can impact the technical infrastructure and operational environments for everyone. Whether or not one considers commercial practices as meriting the same level of concern as, say, data localization is of course a matter of perspective. Certainly there are significant concerns from the perspectives of many Internet users, activists and competing providers in global markets.

As such, the issues are on the table in the growing global dialogue about fragmentation, and they therefore merit consideration here. Accordingly, in this section we briefly survey five sets of issues: peering and standardization; network neutrality; walled gardens; geo-localization and geo-blocking; and infrastructure-related intellectual property protection.

Peering and Standardization

In Section 2, we noted that the complex system of private peering and transit contracts among ISPs has ensured the provision of a stable, integrated global public Internet. The economic models employed in interconnection arrangements historically were based on a "sender keeps all" approach to revenues that contrasted sharply with the regulated and administratively heavy accounting and settlements systems of revenue division used in the traditional telecommunications industry.

With the exponential growth in traffic and other factors, there has been some evolution towards the exchange of payments in some connections. Nevertheless, the system generally has avoided descending into bureaucratization and divisive bargaining over revenues.[64] A concern to keep an eye on, though, is whether the incentives to some operators may change in ways that challenge the system's preservation. For example, one leading observer has argued that, "The incentives to preserve peering, and the broader linkage it promotes across the physical layer, are diminishing," and "changes in the backbone market ... could break down the traditional peering equilibrium."[65]

On a related note, at the ITU's December 2012 World Conference on International Telecommunications (WCIT), the European Telecommunications Network Operators' Association proposed treaty language that would have established a telephony-style "sending party pays" system under which content providers would have to pay to have their information delivered, in addition to their existing fees for connectivity. This would by extension impact inter-carrier relations; as Cerf, Ryan and Senges have concluded, "If adopted,

the proposal would have completely undermined the economic model of the Internet … Such a model would have devastated the openness of the Internet because providers of free content would have had to pay additional fees, effectively increasing the digital divide by forcing economic choices that would benefit only the telecommunications service providers."[66] While the idea was ultimately rejected, *it is not inconceivable that in the future some leading ISPs may seek to change the terms on which they interconnect and are compensated in ways that ultimately could result in fragmentation.*

Another issue to watch is technical standardization. There have long been concerns in the global telecommunications environment about competing and/or proprietary standards being adopted and deployed in ways that limit interconnectivity. And as the Internet becomes ever more central to all global communications, the number and diversity of standards and standards organizations involved in diverse corners of the ecosystem has greatly increased. Some analysts worry that standards blocs could emerge around different organizations and commit to divergent technologies in ways that impact certain uses of the Internet.

An immediate concern relates to the IoT. Appliances of all kinds are being developed with the ability to use the Internet, the web, and wired and wireless access methods to become part of the global Internet. Signs of such a development were evident as early as 2000 when the Ceiva company announced an Internet-enabled picture frame, but the tidal wave of development is rising visibly in this second decade of the 21st Century. Today, planning for the IoT is central to not only the industrial Internet and the digital transformation of industries, but also the digital home and beyond.

Many different industry groups and international organizations are hard at work developing different solutions to IoT standards requirements. Standards competition in the global marketplace is generally a healthy thing, but from standpoints of the users and other players, *the adoption of proprietary standards in key arenas like the IoT could produce fragmenting effects.* As the Internet Society has warned, "A fragmented environment of proprietary IoT technical implementations will inhibit value for users and industry. While full interoperability across products and services is not always feasible or necessary, purchasers may be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, and concern over vendor lock-in … In addition to increasing the costs of standards development, the absence of coordination across efforts could ultimately produce conflicting protocols, delay product deployment, and lead to fragmentation across IoT products, services, and industry verticals."[67]

Network Neutrality

The long-running and globally spreading debate on network neutrality has deeply divided analysts, policy-makers and stakeholders for years. In very

broad terms, it is a debate that has pitted public interest advocates, much of the Internet technical community, and online content providers, on the one hand, against a diverse array of telecommunications and cable network operators and ISPs, on the other. To the former, it is imperative that all data on the Internet be handled in the same non-discriminatory manner, with no variations based on the type of user, content, application, equipment, or mode of communication involved. To the latter, it is more imperative that network providers be able to differentiate along these lines in order to optimally shape traffic, manage network resources and recover the costs of operation so as to be able to continually invest in upkeep and expansion of their networks and services. Policy-makers have been equally divided in their alignments and preferences based on a variety of national conditions.

For the purposes of this paper, we need not delve into the details of this debate, the complexities of which go far beyond what can be captured in a brief characterization such as the above. What matters here is to note that in the view of many keen observers (and not necessarily just net neutrality proponents), there *can be an integral linkage between non-neutral treatment and Internet fragmentation.*

There is certainly no question that some ISPs worldwide have deliberately inhibited some applications. *There have been attempts to wholly block voice over IP (VOIP) or streaming video* either to prevent users from gaining access to alternatives to conventional telephony or to “protect” other users from “excessive” bandwidth consumption. *There also have been efforts to “throttle” bandwidth by slowing peer-to-peer and other applications,* inter alia to regulate network traffic and minimize bandwidth congestion; monetize scarcity by offering quality of services guarantees for preferred uses; or force users to purchase “enhanced” services.

Depending on the circumstances, some of these practices may be among those deemed to violate the net neutrality rules articulated in the US by the Federal Communication Commission, or to violate similar rules in other national or regional jurisdictions. Blocking of this kind can be achieved by dropping packets that reference particular protocols, modifying domain name resolvers to inhibit successful translation of domain names to IP addresses, or mapping the domain names into alternative addresses under the control of the provider of name resolution services.

In a related form of fragmentation, *an ISP might simply interfere with the flow of traffic to or from particular destinations in an attempt to make that access sufficiently unsatisfactory that a user may be compelled to use application services provided by the ISP or others favoured by the ISP.* Such choices by network operators can have significant implications for content creators and Internet users.

A touchstone for the debate on this point was a widely noted 2009 article by Robin S. Lee and Tim Wu. The authors argued that in the United States there is a de facto "zero-price" rule that bans an ISP from charging termination fees to content providers to reach its customers. "The rule also helps avoid the problems of Internet fragmentation, in which content providers who do not reach agreements with ISPs cannot access all customers, and consumers on a single ISP are foreclosed from accessing their content … [changing this] … would inevitably lead to fragmentation – where certain content would only be available on certain service providers – and hence multiple 'Internets'."[68] Other analysts have expanded on the argument by considering the role of online advertising, suggesting that in the absence of the zero-price rule, ISPs would "behave as editors, caring about the profitability of the content they carry. Hence, they have an incentive to induce fragmentation when (i) advertising revenues are potentially large but strongly diminished by competition among CPs, and (ii) contents are not highly valuable and complementary for consumers".[69]

Wherever one stands on net neutrality generally, the question remains: if it occurs that some content providers lose the ability to easily reach some customers and vice versa, does this not increase the levels of fragmentation in informational markets and the public sphere of ideas on the Internet?

Walled Gardens

The practice of erecting "walled gardens" is not new in the realm of electronic communication and information. With the development of the cable television industry came proprietary platforms that offered self-contained user environments. Similarly, with the popularization beyond business of computer networking in the 1980s and 1990s came operations like Prodigy, CompuServe, GENIE, America Online and thousands of Bulletin Board Systems. Reachable by dial-up modems, they were independent of each other and generally did not technologically interwork. As the Internet grew, it became a commonly accessible transport system for users to reach these services and many of the walls eventually came down to allow users inside each garden to reach out to others.

Now with the development of smart mobile devices and the burgeoning "app economy", walled gardens built on propriety platforms have vastly increased in number and diversity and migrated into our pockets. Search engines generally cannot index social and commercial networks like Twitter, Facebook, Snapchat, Amazon, eBay and FLICKR, among others, unless users are logged in. Some services may not be accessible through Internet browsers at all, so the user must use employ the access methods embedded in the mobile apps. Interestingly though, most of them do allow email exchanges so that a comment on a Facebook page, for instance, will show up in the user's email and the user can respond via email as well as logging in to Facebook to respond.

In a walled garden, the application or service provider can have complete control over its own digital space, governing its inhabitants and their behaviour via its Terms of Service. This allows, inter alia, the creation of a secure and stable environment, the promulgation of a distinctive culture and client relationship, and the provision of a high-quality customer experience. It also allows providers to offer exclusive content, "lock in" customers via habits and sunk costs, and gain access to unchallenged long-term revenue streams.

Obviously, a great many users find a good deal of value to "living" in walled gardens. Apple's announcement that in the first week of January 2015 alone customers spent nearly half a billion dollars on apps and in-app purchases, and Facebook's announcement that a billion people used its platform in a single day in August 2015, were clear indications of the widespread loyalty that has been cultivated.

In 2010, *Wired* magazine's former editor-in-chief and a colleague summarized the emerging reality by proclaiming, "The Web is Dead, Long Live the Internet". They noted that, "One of the most important shifts in the digital world has been the move from the wide-open Web to semi-closed platforms that use the Internet for transport but not the browser for display. It's driven primarily by the rise of the iPhone model of mobile computing, and it's a world Google can't crawl, one where HTML doesn't rule. And it's the world that consumers are increasingly choosing, not because they're rejecting the idea of the Web but because these dedicated platforms often just work better or fit better into their lives (the screen comes to them, they don't have to go to the screen). The fact that it's easier for companies to make money on these platforms only cements the trend."[70]

Customer contentment notwithstanding, a growing number of observers have begun to raise concerns about some of the constraints imposed by the gardens and their governance. Leaving aside the grumbles one sometimes hears about the privacy, intellectual property and other policies entailed in some Terms of Service, what is relevant here is the fragmentation of cyberspaces that is thought to accompany the erection of such walls. Digital movement back and forth to the open web environment is limited, searching is limited, and there's nothing comparable to number portability in the telephone world – one usually cannot take one's accumulated digital persona and history or purchased materials to another platform, thus posing a sharp exit vs loyalty trade-off. Hence, from the standpoint of some analyst and stakeholders, *having a growing share of digital life retreat behind companies' walled gardens constitutes a form of fragmentation on the Internet.*

In a somewhat related vein, there is also a debate about *whether the practice of "zero rating" induces fragmentation on the Internet.* Zero-rating is the provision of services that do not incur data costs and are left out of data usage counts. Customers that do not have unmetered subscriptions are able

to access specific sources of content and services free of charge, whether because the ISP covers the costs to attract new customers or is paid by the sponsoring application and service vendors. The precise models used may vary across ISPs and content providers, as well as across countries.[71] But in general, this can be beneficial to lower-income people, particularly in developing countries, who are new to the Internet or whose needs and usage are limited. On the other hand, many observers see this as a form of fragmentation because the user's choices are constrained to a tiny subset of selected Internet sites, applications and services.

Particular attention has been paid in this debate to the Free Basics platform. In cooperation with a half dozen other leading technology companies, Facebook has offering free services to low-income users in 19 (and counting) developing countries. Over 1 billion people are said to have access to these services, and software developers are invited to build products that can take residence on the platform, subject to certain guidelines.

However altruistic the intent may be, this and similar projects have come in for criticism in some online and other spaces like the IGF. The critics charge that zero rating ends up violating net neutrality and favouring the supplier and its selected partners in a manner that limits peoples' access to and understanding of the Internet. Indeed, a coalition of 67 civil society organizations wrote an open letter to Facebook's CEO raising a number of concerns about the project, including that the new users, "could get stuck on a separate and unequal path to Internet connectivity, which will serve to widen – not narrow – the digital divide".[72] Facebook has taken this input on board and made improvements that address some of the concerns, but debate continues with respect to the underlying business model, and consumer uptake in some countries has been uneven.

Finally, it is perhaps relevant to note that some observers worry that Internet users themselves may be taking a cue to erect experiential and socio-cultural walled gardens of their own. In 2002, law professor Cass Sustein made waves by arguing that the Internet fosters social fragmentation by encouraging people to organize into cloistered enclaves of the like-minded where everyone reinforces each other in blocking out unwanted or opposing viewpoints.[73] In 2011, Eli Pariser took the thought further, arguing that corporate algorithms for searching, "liking", "friending" and so forth can have the effect of constructing tightly constraining "filter bubbles" around people that place inconsonant ideas and information out of sight and out of mind.[74] This well-publicized concern has helped to spur the development of a cottage industry of academics and other analysts concerned with the relationships between algorithms and society in general and algorithms and the fragmentation of online identities and social formations in particular. Leaving aside the role of user choice, there are those who would argue that some algorithms could have the effect of limiting and thus fragmenting the

information made available to users. This is a complex matter that would require further consideration than is possible here.

Geo-Localization and Geo-Blocking

Geo-localization is the practice of identifying users' locations by mapping their devices' IP addresses. Companies thus are able to make fine-grained choices about which kinds of content it is acceptable to serve to the user based on his or her geographic location. One result is the geo-targeting of content to users situated in a legally or commercially congenial locality. Another is *geo-blocking, so that the materials in question are rendered inaccessible for access or purchase.* A wide range of companies, particularly in the entertainment industries, have implemented geo-blocking in order to protect intellectual property and licensing relationships with local mass media distribution channels.

In addition, as noted previously, governments may impose geo-blocking requirements to ensure compliance with local laws and customs. Online providers of news and entertainment, gambling services, alcohol and drugs, and so on can thus avoid running afoul of governments abroad. Indeed, some observers argue that the ability to target and constrain access may have beneficial effects from a civil liberties standpoint, since for example controversial forms of speech can be delivered to selected communities without concern for compliance with local community standards elsewhere.[75]

That said, users often claim to find geo-blocking to be frustrating and annoying. Many people seemingly have come to expect that being on the global public Internet should give them full and unfettered access to publicly available content, so they experience the denial of such access as a form of fragmentation. Of course, installing VPN technology generally can circumvent geo-blocking, but this presumes a certain measure of technical facility, decent bandwidth and an ability to pay that may not characterize many user populations. In addition, while IPv4 addresses reportedly can be more accurately located for blocking than IPv6 addresses, the slow diffusion of IPv6 provides the average user with little comfort in this regard.

Importantly, the EC has taken an interest in the potential downsides of geo-blocking for consumers. As part of its work program on the Digital Single Market, the EC is assessing the practice as a barrier to the construction of a border free space with adequate consumer protection. It reports that "74% of the complaints received by the European Consumer Centres Network regarding price differences or other geographical discrimination faced by consumers relate to online cross-border purchases … Sometimes these restrictions on supply and ensuing price differentiation can be justified, for instance where the seller needs to comply with specific legal obligations. However, in many cases online geo-blocking is not justified. These unjustified practices should be expressly prohibited so that EU consumers and

businesses can take full advantage of the single market in terms of choice and lower prices."[76]

Accordingly, the EC plans to make legislative proposals in the first half of 2016 to end what it considers "unjustified" geo-blocking. In parallel, it is considering whether geo-blocking sometimes may be an infringement on EU competition policy. As blocking requirements are often included in contractual and distribution agreements for e-commerce and the licensing of audiovisual content services, the EC is concerned that such practices may constitute illegal barriers to cross-border shopping.

Intellectual Property

The protection of intellectual property rights on the Internet is of course an enormously complex and contested issue-area. The precise governance principles, mix of rights and obligations, treatment of circumvention technologies and modalities of enforcement are just a few of the vast range of issues that have been addressed with respect to copyright, trademark, patents in the Internet environment. Such issues and their relationships to internationally protected rights, such as those enshrined in Article 19 of the Universal Declaration on Human Rights, have been rendered the focus of renewed controversy by the relevant provisions of the TPP deal reached in October 2015, which critics charge constitutes an unbalanced overextension of intellectual property protections on the Internet.[77]

Here again, we need not wade deep into these waters for the purpose of this paper. Our concern is solely with the relationships between certain infrastructure-related techniques of rights protection and Internet fragmentation.

A reasonable baseline from which to depart is offered by the Internet Society's moderate stance that, "The infringement of intellectual property rights is a critical issue that needs to be addressed, but, at the same time, it must be addressed in ways that do not undermine the global architecture of the Internet or curtail internationally recognized rights."[78] Accordingly, it recommends that intellectual property policy processes be conducted in a manner that is multistakeholder and transparent; based on rule of law considerations like due process, equality of rights, fairness, transparency, the right to be heard and legal certainty; and that the "innovation without permission" that made the Internet what it is should be preserved.

There is room for debate as to whether the current mix of national laws and international policy regimes strikes the right balances on these scores. With regard to preserving the Internet's fundamental architecture, some types of fragmentation conceivably could ensue if policies and standards are locked in based on existing technologies rather than being technology neutral.

Similarly, some actions involving the underlying infrastructure could have fragmenting effects.

Consider, for example, the PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, or PIPA) legislation that was introduced in the US Senate in May 2011, and the similar Stop Online Piracy Act (SOPA) legislation that was introduced in the US House of Representatives in October 2011. The two bills provided remedies that varied somewhat in their details, but in general sought to give the US government and copyright holders new abilities to block access to what were deemed "rogue" websites dedicated to the sale of rights infringing or counterfeit goods. Domain name servers were to prevent certain name from resolving to IP addresses of infringing websites, and search engines were to remove or disable their links to such sites.

A variety of concerns were raised about the scope of the blocking, its relationship to questions of freedom expression and fair use, and so on. What matters here is that such laws would have effectively turned the Internet's neutral naming and numbering system into a weapon for blocking content, based on one country's preferences. In addition, they could have inspired a backlash against US position in Internet governance and US firms more generally, or incentivized other countries to adopt similarly constructed laws for whatever local purposes. The legislation did not move forward after a worldwide oppositional campaign on the part of technology companies, civil society activists and others that included coordinated blackouts by Wikipedia, Google and thousands of websites. But *use of the Internet's naming and numbering system to block content arguably would constitute a significant form of fragmentation on the Internet.*

Conclusion

In this section we have highlighted six kinds of current or potential fragmentation related to commercial practices:

1. Potential changes in interconnection agreements
2. Potential proprietary technical standards impeding interoperability in the IoT
3. Blocking, throttling, or other discriminatory departures from network neutrality
4. Walled gardens
5. Geo-blocking of content
6. Potential use of naming and numbering to block content for the purpose of intellectual property protection

5. Conclusions

We have identified 28 examples of current or potential fragmentation of the Internet at both the technical and content and transactions layers. This is admittedly a bit much to digest in order to weigh their respective significance and the necessity of taking steps to redress them. Hence, we would like to suggest a “top 10” set of issues that merit further attention. This is not to suggest that the others we have covered are necessarily less important, although some – most notably of the technical fragmentation variety – may be more bothersome than worrying and/or could well be worked out through efforts already under way. Rather, our 10 comprise cases that are a) fairly pressing or at least worth keeping a close watch of; b) worth examining in greater detail than was possible in this survey; and/or c) potentially amenable to progress through multistakeholder dialogue and collaboration. They are summarized in Table 1, below.

Table 1: 10 Issues to Watch

Issue	Occurrence	Intentionality	Impact	Character
1. Sustained delays or failure to move from IPv4 to IPv6	Potential	No	High, structural	Undesirable
2. Blocking of gTLDs	Current practice	Yes	To be watched	Undesirable
3. Significant alternate root systems	Presently unlikely	Yes	Very high, structural	Very undesirable
4. Filtering and blocking due to content concerns	Current practice	Yes	High	Undesirable
5. Digital protectionism	Current practice	Yes	Can be high	Undesirable
6. Local data processing and/or retention requirements	Current practice	Yes	Can be high	Generally undesirable
7. Prohibitions on the transborder movement of certain categories of commercial data	Current practice	Yes	Can be high	Generally undesirable
8. Strategies for “national Internet segments” or “cybersovereignty”	Current practice	Yes	High, potentially structural	Undesirable
9. Walled gardens	Current practice	Yes	Can be high	Views vary
10. Geo-blocking	Current practice	Yes	Can be high	Views vary

Taking into account these 10 key cases to watch and the preceding discussion, five sets of challenges stand out as being both pressing and

particularly amenable to productive analysis and multi-stakeholder dialogue and cooperation.

Data Localization

The evidence suggests that governments of various stripes are pursuing forms of data localization. The nominal rationales for these courses of action differ across countries. Some governments have said that localization is needed to protect their citizens' personal privacy or insulation from foreign surveillance operations. Others may be motivated by economic development considerations and the expectation that localization will stimulate their domestic industries. An additional concern could be ensuring access to important information that is currently held abroad for the purposes of law enforcement. Whatever the motivations are, the potential costs and benefits of such policies should be carefully assessed based on both conceptual/empirical analyses and consultations with the range of effected stakeholders, including e.g. cloud computing operators, user industries, law enforcement agencies, the technical community and civil society.

Digital Protectionism

Digital trade and protectionism is a broad arena that goes well beyond the question of fragmentation. But one aspect stands out as potentially useful to explore: the application of international trade rules to data flows and localization. For example, the electronic commerce chapter of the TPP agreement contains an Article on Cross-Border Transfer of Information by Electronic Means that requires each government to allow such transfers, including with respect to personal information, when the activity is for the conduct of the business of a covered person. Parties to the agreement can adopt or maintain measures inconsistent with this requirement if these a) are not applied in a manner that would constitute arbitrary or unjustifiable discrimination or a disguised restriction on trade; or b) do not impose restrictions on the transfer of information that are greater than what is needed to achieve the government's objectives. Similarly, the chapter's Article on Location of Computing Facilities states that governments shall not require a covered person to use or locate computing facilities in their territories as a condition for doing business there. Again, governments can adopt or maintain measures inconsistent with this requirement if they meet the tests of a) and b).

How do we assess what measures with respect to data flows or the location of computing facilities meet these tests? Of course, one could simply wait for the agreement to be ratified and tested and for challenges on these grounds to be sorted out by international trade lawyers. But the machinery of dispute settlement will take time, and by then the policies in question could have become entrenched and costly. It could be useful in the meanwhile to have some initial analysis and dialogue between governments and stakeholders

about what actions might constitute arbitrary or unjustifiable discrimination or disguised restrictions on trade; and what actions might exceed what is needed to achieve the government's objectives with respect to restrictions on data flows and the location of facilities.

Access via Mutual Legal Assistance Treaties (MLATs)

One reason that has been cited by some governments for keeping data local is the difficulty faced by Law Enforcement Agencies (LEAs) in obtaining prompt access to critical information held abroad. Many governments say that access is a particular problem with respect to the United States, since the information being sought often is held by US-based technology companies. As a study for the Global Network Initiative points out, "Efficiency is critical so that law enforcement sees MLA as the best way to access data across jurisdictions, rather than demanding data localization or attempting to apply local law extraterritorially."[79]

The widely lamented problem is that the MLAT system is not working efficiently, in part because of constraints imposed by the US Electronic Communications Privacy Act. As one analysis summarizes, "Foreign governments seeking the content of communications (e.g. emails) that are held in another jurisdiction by US-based companies must make government-to-government requests for the data – even if the data is relevant solely for the investigation of local crime. In order to ultimately get the data, they must obtain a warrant from a US judge based on probable cause – a process that takes an average of 10 months. Foreign governments must go through this process even when they are investigating a local crime involving a local victim and a local suspect, and the only connection to the United States is that the data happens to be held by a US firm."[80] Accordingly, the authors of this analysis have proposed a framework for MLAT reform that establishes a series of principles that would allow a government that meets basic human rights, due process standards and transparency standards to get expedited assistance regarding non-US citizens and residents.

Another solution has been advanced by Brad Smith of Microsoft: "We need an international legal framework – an international convention – to create surveillance and data-access rules across borders."[81] Such a convention could supplement the existing MLAT rules. The process could start small by only involving governments that have effective due processes, so as to avoid the system being abused to violate human rights; other governments could subsequently find they have incentives to comply with the standards and join. Whichever approach is followed, it is clear that improving access to data held abroad, particularly by US-based firms, is an important issue to which governments need answers and on which multistakeholder dialogue could be fruitful.

Walled Gardens

In meetings held during the preparation of this paper, World Economic Forum community members expressed a clear interest in further analysis and multistakeholder dialogue on these commercial practices. The applications, platforms and initiatives that have been so labelled by stakeholders and analysts are increasingly integral to daily life, and yet some have faced questions about their business models and implementation. More "deep dive" analysis into the arguments about Internet fragmentation and inclusive dialogue among the relevant stakeholders could help to clarify the issues and more clearly identify win/win opportunities for consideration.

Information Sharing

There are a number of opportunities here to contribute to enhanced policy-making and cooperation on Internet fragmentation and openness. First, there is great variability in the quality of the measurements and data that are available. With regard to technical fragmentation, companies and organizations responsible for managing or coordinating elements of the Internet could provide some pieces of the puzzle, but these may not be formulated and presented in a manner that is readily accessible to non-engineers. With regard to governmental fragmentation, information on individual examples of e.g. filtering, blocking or attack incidents are much easier to come by than systematic data sets revealing current global conditions or patterns. In other cases, it is not clear what "hard numbers" could be devised to capture the actions in question. For commercial fragmentation the same challenges arise; some actions may be detected and measured while others do not lend themselves to this. Any future efforts to "drill down" on particular manifestations of fragmentation and nail down their incidence and costs to different actors or society more generally would thus face challenges that might best be addressed through collaborative networks that monitor and share data.

Support for one recent development could be helpful here. On 18 December 2015, the Internet Engineering Steering Group (which comprises the IETF's chair and area directors) approved publication of "An HTTP Status Code to Report Legal Obstacles".[82] This will become a formal Request for Comment, used by IETF engineers to develop technical standards. At present, when a server returns a "403 Forbidden" HTTP status code, the user probably will not know why access to the desired resource was denied. But the proposed new status code message would return a "451 Unavailable For Legal Reasons" message when the material has been blocked for such reasons (the designation 451 is apparently in honour of the Ray Bradbury, author of the science fiction work, *Fahrenheit 451*). More specific reasons conceivably could be provided as well. This would provide transparency when laws or public policies affect server operations and could be used by websites and

platforms that are forced to block access. Software could crawl the web periodically and aggregate the incidents into publicly accessible online databases.

This paper has provided an overview of current and potential instances of technical, governmental and commercial fragmentation of and on the Internet. The hope is that providing an overview of this complex terrain and its highly variable parts, policy-makers and stakeholders will have a holistic baseline against which to consider in more detail specific instances of fragmentation and the range of options available for their remediation. Being aware of signs of fragmentation bubbling up in the Internet ecosystem is a prerequisite to acting to promote an open Internet in the future.

About the Authors

William J. Drake is an International Fellow and Lecturer in the Institute of Mass Communication and Media Research at the University of Zurich. He is also a member of the Nominating Committee of the Internet Corporation for Assigned Names and Numbers (ICANN); a member of the inaugural Coordination Committee of the NETmundial Initiative; a faculty member of the European and South schools on Internet governance; and an Affiliated Researcher at the Institute for Tele-Information, Columbia University. Previous activities have included serving as a three-term Chair of the NonCommercial Users Constituency, seven-term member of the Board of Directors of the European At Large Organization, and two-term member of the Council of the Generic Names Supporting Organization, in ICANN; a member of the Multistakeholder Advisory Group of the Internet Governance Forum; an expert adviser to the high-level Panel on Global Internet Cooperation and Governance Mechanisms; a member of the UN Working Group on Internet Governance; a member of the Group of High-Level Advisors of UN Global Alliance for ICT and Development; a Vice-Chair and founding Steering Committee member of the Global Internet Governance Academic Network; and an adviser to the World Economic Forum Task Force on the Global Digital Divide. Previous work experience has included: co-editor of the MIT Press book series, *The Information Revolution and Global Politics;* Senior Associate at the Centre for International Governance of the Graduate Institute of International and Development Studies; President of Computer Professionals for Social Responsibility; Senior Associate and Director of the Project on the Information Revolution and World Politics at the Carnegie Endowment for International Peace; founding Associate Director of the Communication, Culture and Technology Program, Georgetown University; Assistant Professor of Communication at the University of California, San Diego; and adjunct professor at the School of Advanced International Studies and the Georgetown School of Business. He holds a PhD in Political Science from Columbia University. www.williamdrake.org

Vinton G. Cerf is Vice-President and Chief Internet Evangelist for Google. He is responsible for identifying new enabling technologies and applications on the Internet and other platforms for the company. Widely known as a “father of the Internet”, Vint is the co-designer with Robert Kahn of TCP/IP protocols and basic architecture of the Internet. In 1997, President Clinton recognized their work with the US National Medal of Technology. In 2005, Vint and Bob received the highest civilian honour bestowed in the United States, the Presidential Medal of Freedom. From 1994-2005, Vint served as Senior Vice-president at MCI. Prior to that, he was Vice-president of the Corporation for National Research Initiatives, and from 1982-86 he served as Vice-president of MCI. During his tenure with the US Department of Defense's Advanced Research Projects Agency from 1976-1982, Vint played a key role leading the development of Internet and Internet-related data packet and security technologies. From 2000-2007, Vint served as chairman of the board of the

Internet Corporation for Assigned Names and Numbers and he has been a Visiting Scientist at the Jet Propulsion Laboratory since 1998. He served as founding president of the Internet Society from 1992-1995 and was on its board until 2000. Vint is a Fellow of the IEEE, ACM, AAAS, the American Academy of Arts and Sciences, the International Engineering Consortium, the Computer History Museum and the National Academy of Engineering. Vint has received numerous awards and commendations in connection with his work on the Internet, including the Marconi Fellowship, Charles Stark Draper award of the National Academy of Engineering, the Prince of Asturias award for science and technology, the Alexander Graham Bell Award presented by the Alexander Graham Bell Association for the Deaf, the A.M. Turing Award from the Association for Computer Machinery, the Silver Medal of the International Telecommunications Union, and the IEEE Alexander Graham Bell Medal, among many others. He holds a Ph.D. in Computer Science from UCLA and more than a dozen honorary degrees.
http://research.google.com/pubs/author32412.html

Wolfgang Kleinwächter is a Professor Emeritus for International Communication Policy and Regulation from the University of Aarhus in Denmark. He also is a former member of the Internet Corporation for Assigned Names and Numbers' (ICANN) Board of Directors and Special Ambassador of the NETmundial Initiative. He has been involved in Internet governance issues since the early 1990s. He was a member of the UN Working Group on Internet Governance, a Special Adviser to the chair of the Internet Governance Forum (2005-2010) and a member of the UNCSTD IGF Improvement Working Group (2010-2012). He has been involved in ICANN since 1998 where he chaired, inter alia, the Nominating Committee and was a member of the GNSO Council. He is also a co-founder of the European Dialogue on Internet Governance, the Global Internet Governance Academic Network, and the ICANN Studienkreis. In 2009 the Council of Europe appointed him to chair the Cross Border Internet Expert Group. He also chaired the Internet Governance Sub-Group of the EU Task Force on the Internet of Things and the evaluation team of EUs Safer Internet Action Program. In the academic world, Wolfgang Kleinwächter was from 1988 to 2012 member of the International Council of the International Association for Media and Communication Research, in which for more than 10 years he chaired the IAMCR Law Section. From 1994-1998 he chaired the Coordination Committee of the European Interregional Information Society Initiative. From 2007 to 2012 he was a member of the Steering Board of the EU FP 7 "Next Generation Internet/EURO-NF" research project. He is the founder and chair of the European Summer School on Internet Governance, and has testified in hearings in the Deutsche Bundestag and the European Parliament and has published and edited more than 200 articles and 12 books. In 2012 he received the Internet Award by the German Internet Economy Association (eco). https://www.icann.org/profiles/wolfgang-kleinwachter

Acknowledgements

In 2015, on the onset of the Future of the Internet Global Challenge Initiative, the World Economic Forum recognized the concern about fragmentation as it relates to the future development of the Internet. Under the leadership of William J. Drake, International Fellow and Lecturer at the University of Zurich, *Internet Fragmentation: An Overview* is a baseline paper that examines the current state of play of the various forms of fragmentation affecting the Internet. Along with co-authors Vint Cerf, a “father of the Internet”, and Wolfgang Kleinwächter, Professor Emeritus at the University of Aarhus, William J. Drake, in partnership with the World Economic Forum, drafted this paper as one of the major outcomes for the first year of the Governance on the Internet workstream of the overall Initiative. The World Economic Forum team that assisted in the production of the paper includes Richard Samans, Mark Spelman, Alex Wong, Danil Kerimi, Mara Kelly and Alexandra Shaw.

For their helpful written and oral comments on the first draft of the paper, the authors and the World Economic Forum wish to thank:

Nora Abusitta, ICANN
Fiona Alexander, US Department of Commerce
Anupam Chander, University of California, Davis
Leslie Daigle, Thinking Cat
Bertrand de la Chapelle, Internet and Jurisdiction Project
Eileen Donahoe, Human Rights Watch
Anriette Esterhuysen, Association for Progressive Communications
Urs Gasser, Harvard University
Merit E. Janow, Columbia University
Jānis Kārkliņš, Internet Governance Forum
Judith Lichtenberg, The Global Network Initiative
Mats Nilsson, Ericsson
Burke Norton, Salesforce
Sundeep Oberoi, Tata Consultancy Services
Robert Pepper, Cisco
Christoph Steck, Telefonica
Sacha Wunsch-Vincent, World Intellectual Property Organization
Jonathan Zittrain, Harvard University

Endnotes

[1] For an elaboration of this vision, see, Schwab, Klaus, “The Fourth Industrial Revolution: What It Means and How to Respond”, *foreignaffairs.com,* 12 December 2015, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

[2] Gasser, Urs, and Palfrey, John G., Interop: The Promise and Perils of Highly Interconnected Systems. Basic Books, 2012. For further explorations of the concept, see https://cyber.law.harvard.edu/research/interoperability.

[3] Huston, Geoff, “Thoughts on the Open Internet - Part 2: The Where and How of "Internet Fragmentation”, *CircleID,* 6 October 2015, p.1, http://www.circleid.com/posts/20151006_open_internet_part_2_where_and_how_of_internet_fragmentation.

[4] “Internet Invariants: What Really Matters”, *The Internet Society,* 3 February 2012, pp.1 & 2, http://www.internetsociety.org/sites/default/files/Internet%20Invariants-%20What%20Really%20Matters.pdf. For a detailed analysis relating these invariants to fragmentation, see, Daigle, Leslie, “On the Nature of the Internet”, *Global Commission on Internet Governance, Paper Series: No. 7,* March 2015, https://www.cigionline.org/publications/nature-of-internet.

[5] Zittrain, Jonathan, *The Future of the Internet And How to Stop It*, Yale University Press, 2008, p.70.

[6] Jonah Force Hill adopts a layered approach to explore six case studies arrayed across what he calls the physical, logical, information and people layers. See, Force Hill, Jonah, "Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers”, *Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs,* Harvard Kennedy School, May 2012, http://belfercenter.ksg.harvard.edu/files/internet_fragmentation_jonah_hill.pdf.

[7] *Report of the Working Group on Internet Governance,* Château de Bossey, Switzerland, June 2005, p. 4.

[8] See, inter alia, Drake, William J., “Conclusion: Why the WGIG Process Mattered”, in *Reforming Internet Governance: Perspectives from the UN Working Group on Internet Governance,* edited by William J. Drake, pp. 249-265, United Nations Information and Communication Technologies Task Force, 2005, http://www.wgig.org/docs/book/WGIG_book.pdf; and, Kleinwächter, Wolfgang, “Sharing Decision Making in Internet Governance: The Impact of the WGIG Definition”, in *The Working Group on Internet Governance: 10th Anniversary Reflections,* edited by William J. Drake, pp. 66-

88, Association for Progressive Communications, 2015, https://www.apc.org/en/WGIG

[9] For contrasting views on the merits of this common terminology, see, Drake, William J., "Reframing Internet Governance Discourse: Fifteen Baseline Propositions", in *Internet Governance: A Grand Collaboration,* edited by Don MacLean, United Nations Information and Communication Technology Taskforce, 2004, at pp. 126-127; and de la Chapelle, Bertrand, "The Internet Governance Forum: How a United Nations Summit Produced a New Governance Paradigm for the Internet Age", in *Governing the Internet, Freedom and Regulation in the OSCE Region,* edited by Christian Möller and Arnaud Amouroux, OSCE, 2007, at p. 22.

[10] Legal fragmentation is mentioned in Global Commission on Internet Governance, *Research Advisory Network Paris Meeting, 27 June 2014,* https://ourinternet.org/event/global-commission-on-internet-governance-research-advisory-network-paris-meeting; and Jardine, Eric, "Should the Average Internet User in a Liberal Democracy Care About Internet Fragmentation?" *Centre for International Governance Innovation,* 19 September 2014, https://www.cigionline.org/print/blogs/reimagining-internet/should-average-internet-user-liberal-democracy-care-about-internet-fragme. For a detailed discussion of the challenges posed by differences in legal systems, see, Weber, Rolf H., "Legal Interoperability as a Tool for Combatting Fragmentation", *Global Commission on Internet Governance, Paper Series: No. 4,* December 2014, https://www.cigionline.org/sites/default/files/gcig_paper_no4.pdf.

[11] Noam, Eli M., "Towards a Federated Internet", *InterMEDIA,* vol. 41, no. 4, 2013, pp. 10 & 12.

[12] The IANA functions historically have included the coordination of the assignment of technical IP parameters; the administration of responsibilities associated with Internet DNS root zone management; the allocation of Internet numbering resources; and other services related to the management of the .ARPA and .INT top-level domains. For details, see, http://www.iana.org and https://www.icann.org/stewardship.

[13] For more information, see, https://www.nro.net/about-the-nro/regional-internet-registries.

[14] For example, it has recently been reported that over 10% of users connecting to Google's sites are coming in over IPv6. See, Dan York, "Global IPv6 Deployment Now Passes 10%!" *CircleID,* 4 January 2015, http://www.circleid.com/posts/20160104_global_ipv6_deployment_now_passes_10/.

[15] For a discussion, see, Chertoff, Michael, and Tobby Simon, “The Impact of the Dark Web on Internet Governance and Cyber Security”, *Global Commission on Internet Governance Paper Series no. 6,* February 2015, https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

[16] https://newgtlds.icann.org/en/program-status/delegated-strings.

[17] Updated figures on the progress of the New gTLD Program are available at, https://newgtlds.icann.org/en/program-status/statistics.

[18] VeriSign, Inc. Quarterly Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Quarterly Period ended September 30, 2015, 16 October 2015, http://www.sec.gov/Archives/edgar/data/1014473/000101447315000073/vrsn-2015930x10q.htm. Emphasis added.

[19] Huston, Geoff, “What's in a Name?” *The ISP Column,* December 2015, http://www.potaroo.net/ispcol/2015-12/names.html.

[20] *Yeti DNS Project,* http://www.yeti-dns.org/.

[21] “Overview of the Digital Object Architecture”, *Corporation for National Research Initiatives,* 28 July 2012, http://www.cnri.reston.va.us/papers/OverviewDigitalObjectArchitecture.pdf.

[22] Diffie, W. and M. Hellman, "New Directions in Cryptography”, *IEEE Transactions on Information Theory*, vol. 22, no. 6, 1975, pp. 644–654, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=1055638.

[23] See, *The DNSSEC Deployment Initiative,* http://www.dnssec-deployment.org.

[24] The terminology is problematic in several senses and will not otherwise be used here. For discussions, see, respectively, Alves Jr., Sergio, “Internet Governance 2.0.1.4: The Internet Balkanization Fragmentation”, 29 June 2014, http://ssrn.com/abstract=2466222; and Maher, Katherine, “The New Westphalian Web”, *Foreign Policy,* 25 March 2013, http://foreignpolicy.com/2013/02/25/the-new-westphalian-web. For a terminological corrective, see, Maurer, Tim, and Robert Morgus, “Stop Calling Decentralization of the Internet ‘Balkanization,’” *Slate*, 19 February 2014, http://www.slate.com/blogs/future_tense/2014/02/19/stop_calling_decentralization_of_the_internet_balkanization.html?wpisrc=burger_bar.

[25] See, for example, Kahin, Brian, and Charles Nesson (eds), *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, MIT

Press, 1997. For a more recent treatments emphasizing the battles over global governance, see, inter alia, Mueller, Milton L., *Networks and States: The Global Politics of Internet Governance*, MIT Press, 2010; and DeNardis, Laura, *The Global War for Internet Governance,* Yale University Press, 2014.

[26] For an overview of the historical evolution of these international regimes and the role of sovereignty therein, see, Drake, William J., "Introduction: The Distributed Architecture of Network Global Governance", in *Governing Global Electronic Networks: International Perspectives on Policy and Power,* edited by William J. Drake and Ernest J. Wilson III, pp. 1-78, MIT Press, 2008.

[27] Werbach, Kevin, "Digital Tornado: The Internet and Telecommunication Policy", *Federal Communications Commission, OPP Working Paper Series No. 29,* March 1997, https://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf.

[28] The zeitgeist of the time was reflected in such popular works as, Cairncross, Frances, *The Death of Distance: How the Communication Revolution Is Changing Our Lives*, Harvard Business School Press, 1997.
[29] United Nations, *The Universal Declaration of Human Rights,* http://www.un.org/en/universal-declaration-human-rights.

[30] International Telecommunication Union, Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference, 2011 Edition, ITU, 2011, p. 37, http://www.itu.int/dms_pub/itu-s/oth/02/09/S02090000115201PDFE.PDF.

[31] There are many surveys available of the range and diversity of Internet regulations and censorship. A few excellent specialized sites for the cross-national tracking of these developments include http://www.giswatch.org/, https://opennet.net, https://rankingdigitalrights.org/, and https://thenetmonitor.org.

[32] Deibert, Ronald, and Rafal Rohozinski, "Beyond Denial: Introducing Next-Generation Information Access Controls", in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, edited by Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain, MIT Press, 2009, p. 7. For more details, see http://access.opennet.net.

[33] For a discussion of the issues, see, Organization for Economic Cooperation and Development, "Measuring the Internet Economy: A Contribution to the Research Agenda", *OECD Digital Economy Paper No. 226,* OECD, 2013, http://www.oecd-ilibrary.org/science-and-technology/measuring-the-internet-economy_5k43gjg6r8jf-en.

[34] Zwillenberg, Paul, Dominic Field and David Dean, *Greasing the Wheels of the Internet Economy,* The Boston Consulting Group, January 2014, https://www.icann.org/en/system/files/files/bcg-internet-economy-27jan14-en.pdf p. 6.

[35] See, for example, Dalberg Global Development Advisors, *Open for Business? The Economic Impact of Internet Openness,* March 2014, http://www.dalberg.com/documents/Open_for_Business_Dalberg.pdf. The authors express skepticism though as to whether the economic impact can be fully captured in terms of growth in Gross Domestic Product.

[36] See, for example, Aldonas, Grant D. and Usman Ahmed, "Addressing Barriers to Digital Trade", *The E15 Initiative,* December 2015, http://e15initiative.org/publications/addressing-barriers-to-digital-trade/; as well as the related papers from this initiative co-convened by the World Economic Forum and the International Centre for Trade and Sustainable Development, http://e15initiative.org/themes/digital-economy.

[37] Schaake, Marietje, et al., "Statement on 'Digital Protectionism,'" Brussels, 22 September 2015, http://www.marietjeschaake.eu/wp-content/uploads/2015/09/2015-09-22-MEPs-Statement-on-Digital-Protectionism.pdf.

[38] The travails of the Work Programme's efforts since 1998 to sort out the application of WTO disciplines to the online world are discussed in Drake, William J., and Kalypso Nicolaïdis, "Global Electronic Commerce and GATS: The 'Millennium Round' and Beyond", in *GATS 2000: New Directions in Services Trade Liberalization,* edited by Pierre Sauve and Robert M. Stern, pp. 399-437, The Brookings Institution Press, 2000; Wunsch-Vincent, Sacha, *The WTO, the Internet and Trade in Digital Products: EC-US Perspectives,* Hart Publishing, 2006; and, Burri, Mira, and Thomas Cottier (eds.) *Trade Governance in the Digital Age: World Trade Forum*, Cambridge University Press, 2012.

[39] The apt term is coined in Zwillenberg, Paul, Dominic Field and David Dean, *op. cit.,* 2014.

[40] For a concise overview, see, Vaidya, Tavish, "2001-2013: Survey and Analysis of Major Cyberattacks", Department of Computer Science, Georgetown University, July 2015, http://arxiv.org/pdf/1507.06673.pdf. More detailed information is available from the NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/index.html.

[41] "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", *Sixty-sixth session of the*

United Nations General Assembly, A/66/359, 14 September 2011, pp. 4-5, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf. Emphasis added.

[42] Members States of the Group of 77 and China, *op cit.,* p. 8.

[43] For a discussion, see, Gassman, Hans-Peter, and G. Russell Pipe, ‘‘Synthesis Report,’’ in *Policy Issues in Data Protection and Privacy: Concepts and Perspectives—Proceedings of the OECD Seminar 24th to 26th June 1974,* pp. 12–41, Organization for Economic Cooperation and Development, 1976.

[44] Kuner, Christopher, “Data Nationalism and its Discontents”, *Emory Law Journal,* v. 64, 2015, pp. 2089-2098, http://law.emory.edu/elj/_documents/volumes/64/online/kuner.pdf.

[45] Force Hill, Jonah, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders.” 3. *Lawfare Research Paper Series,* 21 July 2014, https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf.

[46] For an overview, see, Drake, William J., “Territoriality and Intangibility: Transborder Data Flows and National Sovereignty”, in Kaarle Nordenstreng and Herbert I. Schiller, eds., *Beyond National Sovereignty: International Communications in the 1990s,* Ablex Press, 1993, pp. 259-313.

[47] Some of these measures are discussed in United Nations Centre on Transnational Corporations, *Transnational Corporations and Transborder Data Flows: A Technical Paper,* UNIPUB, 1982.

[48] Rothrock, Kevin, “Russia Says Twitter Doesn’t Need to Comply With Its New Data-Localization Law”, *Global Voices Advocacy,* July 2015, https://advocacy.globalvoicesonline.org/2015/07/23/russia-says-twitter-doesnt-need-to-comply-with-its-new-data-localization-law/.

[49] Olivia Solon, “Russia’s Fist Just Clenched Around the Internet a Little Tighter”, *Bloomberg.com,* 31 August 2015, http://www.bloomberg.com/news/articles/2015-08-31/russia-internet-law-tests-facebook-google-and-other-foreign-firms.

[50] Greenleaf, Graham and George Tian, “China Expands Data Protection through 2013 Guidelines: A ‘Third Line’ for Personal Information Protection (With a Translation of the Guidelines)”, *Privacy Laws & Business International Report,* no. 122, April 2013, pp.1 & 5, http://ssrn.com/abstract=2280037.

[51] Paul Mozur, “China Tries to Extract Pledge of Compliance From U.S. Tech Firms”, *The New York Times,* 16 September 2015, http://www.nytimes.com/2015/09/17/technology/china-tries-to-extract-pledge-of-compliance-from-us-tech-firms.html.

[52] Lulu Yilun Chen, “China to Set Up ‘Security Offices’ Inside Internet Companies”, *Bloomberg.com,* 5 August 2015, http://www.bloomberg.com/news/articles/2015-08-05/china-to-set-up-security-offices-inside-internet-companies.

[53] For surveys of these trends see, Chander, Anupam and Uyen P. Le, “Data Nationalism”, *Emory Law Journal,* v. 64, 2015, pp. 677-739, http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf; Maurer, Tim, Robert Morgus, Isabel Skierka and Mirko Hohmann, “Technological Sovereignty: Missing the Point?” in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace,* edited by M. Maybaum, A.-M. Osula, and L. Lindstroom, pp. 53-68, NATO CCD COE Publications, 2015; and Force Hill, Jonah, op. cit.

[54] Castro, Daniel, “The False Promise of Data Nationalism”, *The Information Technology & Innovation Foundation,* p. 1, December 2013, http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

[55] Chander and Le, *op. cit.,* pp. 721 & 722.

[56] Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde, “The Costs of Data Localisation: Friendly Fire on Economic Recovery”, European Centre for International Political Economy, *ECIPE Occasional Paper No. 3,* 2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

[57] Ezell, Stephen, Robert D. Atkinson, and Michelle Wein, “Localization Barriers to Trade: Threat to the Global Innovation Economy”, *The Information Technology & Innovation Foundation,* 25 September 2013, https://www.copyrightalliance.org/sites/default/files/resources/2013-localization-barriers-to-trade.pdf.

[58] Members States of the Group of 77 and China, “Written Submission to the Draft Final Document of the UNGA High-Level Meeting on the Implementation of WSIS Outcomes”, undated, pp. 6, 9 & 10. Emphasis added.

[59] Russian Federation, “Written Submission to the Draft Final Document of the UNGA High-Level Meeting on the Implementation of WSIS Outcomes”, undated, p. 3. Emphasis added.

[60] "Highlights of Xi's Internet Speech", 16 December 2015, http://www.wuzhenwic.org/2015-12/16/c_47742.htm.

[61] Chehadé, Fadi, "If We Fragment The Internet, 'It Will Not Be The Internet As We Know It,'" *The Huffington Post,* 24 January 2014, http://www.huffingtonpost.com/2014/01/24/fadi-chehade-davos_n_4635949.html.

[62] *NETmundial Multistakeholder Statement,* April, 24th 2014, p. 5 http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf. For assessments of the meeting and the roadmap, see, Drake, William J. and Monroe Price (eds.), *Internet Governance: The NETmundial Roadmap,* USC Annenberg Press, 2014.

[63] Kaspersky, Eugene, "What Will Happen if Countries Carve Up the Internet?" *The Guardian,* Tuesday 17 December 2013, http://www.theguardian.com/media-network/media-network-blog/2013/dec/17/internet-fragmentation-eugene-kaspersky.

[64] For a useful overview, see, Kovacs, Anna-Maria, "Internet Peering and Transit", *Technology Policy Institute,* 4 April 2012, https://www.techpolicyinstitute.org/files/amkinternetpeeringandtransit.pdf.

[65] Werbach, Kevin, "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart", *University of California Davis Law Review,* vol. 42, 2008-2009, p.370. http://lawreview.law.ucdavis.edu/issues/42/2/articles/42-2_Werbach.pdf.

[66] Cerf, Vinton G. and Ryan, Patrick S. and Senges, Max, "Internet Governance Is Our Shared Responsibility", *I/S: A Journal of Law and Policy for the Information Society,* vol. 10, n. 1, 2014, pp. 21-22. http://ssrn.com/abstract=2309772.

[67] The Internet Society, *The Internet of Things (IoT): An Overview,* 15 October 2015, pp. 2 & 22. http://www.internetsociety.org/doc/iot-overview.

[68] Lee, Robin S. and Tim Wu, "Subsidizing Creativity through Network Design: Zero-Pricing and Net Neutrality", *Journal of Economic Perspectives,* vol. 23, no. 3, Summer 2009, pp. 75 & 67, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1489166.

[69] D'Annunzio, Anna and Antonio Russo, "Net Neutrality and Internet Fragmentation: The Role of Online Advertising", *International Journal of Industrial Organization* vol. 43, 2015, pp. 30-47, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2643357.

[70] Anderson, Chris and Michael Wolff, “The Web is Dead. Long Live the Internet”, *Wired,* 17 August 2010, http://www.wired.com/2010/08/ff_webrip.

[71] For empirical evidence of the variations, see, Rossini, Carolina and Taylor Moore, *Exploring Zero Rating Challenges: Views From Five Countries,* Public Knowledge, 28 July 2015, https://www.publicknowledge.org/documents/exploring-zero-rating-challenges-views-from-five-countries.

[72] Access, et al., “Open Letter to Mark Zuckerberg Regarding Internet.org, Net Neutrality, Privacy, and Security”, *Facebook,* 18 May 2015 https://www.facebook.com/notes/accessnoworg/open-letter-to-mark-zuckerberg-regarding-internetorg-net-neutrality-privacy-and-/935857379791271.

[73] Sunstein, Cass R., *Republic.com,* Princeton University Press, 2002.

[74] Pariser, Eli, The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think, Penguin Books 2012.

[75] See, Kjar, J. Mason, “2 Obscenity Standards, 1 Neat Solution: How Geotargeting Extends Traditional Obscenity Law to the Internet”, *Case Western Reserve Journal of Law, Technology & the Internet,* 125, 2012, http://ssrn.com/abstract=1808307.

[76] European Commission, “A Digital Single Market Strategy for Europe”, Communication from the Commission to the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2015) 192 final, Brussels 5 May 2015, p. 6, https://ec.europa.eu/digital-agenda/en/news/digital-single-market-strategy-europe-com2015-192-final.

[77] For contending views on this aspect of the agreement, see for example, Weatherall, Kimberlee G., "Section by Section Commentary on the TPP Final IP Chapter Published 6 November 2015 – Part 1 – General Provisions, Trade mark, GIs, Designs”, 7 November 2015, http://works.bepress.com/kimweatherall/31; Weatherall, "Section by Section Commentary on the TPP Final IP Chapter Published 5 November 2015 – Part 2 – Copyright”, 7 November 2015, http://works.bepress.com/kimweatherall/32; and, “Statement from MPAA Chairman and CEO Senator Chris Dodd on the Successful Conclusion of the TPP Negotiations”, Motion Picture Association of America, 5 October 2015, http://www.mpaa.org/wp-content/uploads/2015/10/Statement-from-MPAA-Chairman-and-CEO-Senator-Chris-Dodd-on-the-Successful-Conclusion-of-the-TPP-Negotiations.pdf.

[78] Komaitis, Konstantinos, “Internet Society Issues Paper on Intellectual Property on the Internet”, *The Internet Society,* 13 June 2013, p. 2, http://www.internetsociety.org/doc/internet-society-issues-paper-intellectual-property-internet.

[79] Woods, Andrew K., *Data Beyond Borders: Mutual Legal Assistance in the Internet Age,* Global Network Initiative, January 2015, p. 7, https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf.

[80] Daskal, Jennifer and Andrew K. Woods, “Cross-Border Data Requests: A Proposed Framework”, *Just Security*, 24 November 2015, https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework.

[81] Brad Smith, “Time for an International Convention on Government Access to Data”, *Microsoft.com,* 20 January 2014, http://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data.

[82] Bray, T., “An HTTP Status Code to Report Legal Obstacles draft-ietf-httpbis-legally-restricted-status-04”, *Internet Engineering Task Force, HTTP Working Group*, Internet-Draft, 10 November 2015, https://tools.ietf.org/html/draft-ietf-httpbis-legally-restricted-status-04.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org